高职高专计算机系列教材

主编　谭浩强

网络管理基础

实用教程



清华大学出版社

高职高专计算机系列教材

主编　谭浩强

网络管理基础

尚晓航　编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书从系统管理员的角度出发,结合中小型 Intranet 的建设和管理中的具体实例和要求,系统地讲解了网络管理的基础知识以及网络管理员在规划、设计、实现和管理 Intranet 时所必备的基本知识和实用操作技能。

本书的特点是既有适度和必要的基础理论知识介绍,又有比较详细的 Intranet 建设和 NT 网络管理的实用技术指导,并力求反映最新的网络管理技术。书中配有大量实例和插图,内容深入浅出。每章后面附有大量习题及实验项目的建议。

本书适合作为各类高职高专院校的教材,也可作为在职技术人员的自学参考书。

图书在版编目(CIP)数据

网络管理基础/尚晓航编著.—北京:清华大学出版社,2002
高职高专计算机系列教材
ISBN 7-302-06005-3

Ⅰ.网… Ⅱ.尚… Ⅲ.计算机网络—管理—高等学校:技术学校—教材 Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字(2002)第 081673 号

出版者: 清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者: 北京国马印刷厂
发行者: 新华书店总店北京发行所
开　本: 787×1092 1/16　**印张:** 22　**字数:** 503 千字
版　次: 2002 年 12 月第 1 版　2002 年 12 月第 1 次印刷
书　号: ISBN 7-302-06005-3/TP • 3582
印　数: 0001～6000
定　价: 28.00 元

编辑委员会



《高职高专计算机系列教材》

到21世纪,计算机将成为人类的常用现代工具,每一个有文化的人都应当了解计算机,学会使用计算机,并用它来处理面临的事务。

学习计算机知识有两种不同的方法:一种是侧重知识的学习,从原理入手,注重理论和概念;另一种是侧重应用的学习,从实际入手,注重掌握其应用方法和技能。不同的人应根据其具体情况选择不同的学习方法。对多数人来说,计算机是作为一种工具来使用的,主要以应用为目的,以应用为出发点。对于高职和高专的学生,显然应当采用后一种学习方法。

传统的理论课程采用以下的三部曲:提出概念——解释概念——举例说明,这适合前面第一种方法。对于侧重应用的学习者,我们在教学实践中摸索出新的三部曲:提出问题——介绍解决问题的方法——最后归纳出一般规律或概念。实践证明这种方法是行之有效的,减少了初学者在学习上的困难。传统的方法是:先理论后实际,先抽象后具体,先一般后个别。我们采用的方法是:从实际到理论,从具体到抽象,从个别到一般,从零散到系统。我们认为,后一种方法对高职、高专和成人高教是很合适的。

本系列教材是针对高职和高专的特点组织编写的,包括了高职高专的计算机专业和非计算机专业的教材和参考书。不同专业可以从中选择所需的部分。本系列教材包含的内容比较广,除了可作为正式教材外,还可作为某些专业的选修课或指定自学的教材。

应当指出,检查学习好坏的标准,不是"知道不知道",而是"会不会用",学习的目的全在于应用。因此,希望读者一定要重视实践环节,多上机练习,千万不要满足于"上课能听懂、教材能看懂"。有一些问题,别人讲半天也不明白,自己一上机就清楚了。教材中有些实践性比较强的内容,不一定在课堂上由老师讲授,而应指定学生通过上机掌握。这样做可以培养学生的自学能力,启发学生的求知欲望。

本系列教材是由"浩强创作室"组织北京和天津一些普通高校和高职大学的老师们编写的,他们对高职高专的教学特点有较多的了解,有较多的实践经

验。相信本系列教材的出版会有助于高职高专的教材建设和教学改革。

由于我国的高职教育正在蓬勃发展,许多问题有待深入讨论,新的经验将会层出不穷,对如何进行高职教育将会有更新更深入的认识,本系列教材的内容也将会不断丰富和调整。我们只是为了满足许多高职高专学校对教材的急需,才下决心抓紧编写了这套系列教材,以期抛砖引玉。清华大学出版社克服了许多困难,使本系列教材在较短的时间内得以出版。

本系列教材肯定会有不足之处,请专家和读者不吝指正。

欢迎访问谭浩强网站:http://www.tanhaoqiang.com。

《高职高专计算机系列教材》主编

全国高等院校计算机基础教育研究会理事长

谭浩强

1999 年 11 月 1 日



目前，计算机网络正在越来越多的领域中得到推广和应用，政府、公司、学校等各个部门和单位的计算机网络化已经成为计算机发展的必然。另外，计算机网络也是支持全球信息基础结构的最主要技术之一，国内外的信息技术和信息产业都需要大量掌握计算机网络技术、通信技术和网络管理技术的专门人才。因此，计算机网络技术和计算机网络操作系统，不但是计算机及其相关专业的学生应当重点学习和掌握的重要课程，也是非计算机专业的学生应当学习的课程，更是从事计算机网络应用的人员应当掌握的重要知识之一。

网络管理集通信技术和网络技术于一体，通过调度和协调资源，进行配置管理、故障管理、性能管理、安全维护和计费管理等，达到网络可靠、安全和高效运行的目的。在网络技术迅速发展的今天，网络管理已成为当今社会中的热门技术，不但是网络应用专业学生的一门重要必修课，也是许多相关专业学生的选修课。

本书作者曾在某外企担任计算机部主管，并出国进修计算机仿真技术一年。近年来，由于教学工作需要，曾在北京联合大学计算机信息自动化专业、办公自动化专业以及计算机网络应用专业的学生中，开设“计算机局域网与Windows NT 实用组网技术”、“网络管理与维护技术”、“计算机网络与通信技术”和“组网技术”等课程，均受到学生的普遍欢迎。本书就是作者结合实际工作的经验和教学的体会，以及我校在组网方面的实践经验编写而成的。本书从实用性出发，结合管理一个公司、企业信息网络的实际经验，对具体的网络集成技术、组网技术、信息网站的建设、网络管理和维护、数据保护和网络安全技术等方面进行了详细的阐述，其目的在于为读者提供组网的实验指导，使读者可以利用该教材设计、组建和管理好自己的网络。

本书的读者既可以是有一定计算机网络基础知识和网络管理经验的人员，也可以是打算建设小型网络的新手。对于前者，由于需要更全面地掌握网络管理的知识和技能，因此，应当先学习《网络技术基础》和《Internet 基础》的有关理论知识和组网技术，再依次学习本书各章的内容。而对于后者，读者可

能尚未学习过上述课程，由于只打算设计和建立好一个小型网络，因此，可以直接从第 6 章开始学习，进而逐步掌握一个实用网络的设计、建设和管理的全部过程。

本书共 16 章，分为以下几个部分，详细地介绍了网络系统管理中需要的基本概念、基本知识和操作技能。

第 1 部分：第 1 章～第 5 章为“网络管理的基础篇”。主要介绍了网络管理的基本概念以及网络系统集成的相关知识和技术。包括：局域网与广域网的互联与接入技术，Internet、Intranet、Extranet、局域网的基本知识，网络系统集成的概念、步骤与应用等，以及在 Intranet 规划、设计和建设过程中所需要的系统知识。

第 2 部分：第 6 章～第 13 章为“NT 网络的基本管理篇”。包括Windows NT 网络系统的设计、安装、配置和卸载、网络中的 TCP/IP 管理、网络用户的组织与优化管理、网络中计算机和共享资源的管理、网络的打印管理、Intranet 信息网站的建设与管理和远程访问服务和电子邮件管理等各种实用管理技术。这部分内容是网络管理员在组建和管理 NT 网络时必须深刻理解和熟练掌握的。

第 3 部分：第 14 章和第 15 章为“网络的数据保护和安全管理篇”。在这一部分中，进一步深入地介绍了管理 Intranet 网络所需的更深层次的知识和操作技能。主要包括网络中的数据保护与系统恢复技术和网络安全管理方面的内容。这部分内容为管理一个实际的 Intranet 不可缺少的内容，也是网络管理员管理一个中型的 NT 信息网络必须掌握的基础知识和必备的操作技能。

第 4 部分：第 16 章“网络管理员的职责综述”。在这一部分中，通过一个综合性的网络建设和管理案例，综述了网络管理员的工作目标和基本职责。使得读者在学习了本书各章内容之后能够对网络管理的日常工作和具体内容有一个概括性的总结和认识。

本书实验环境的要求如下：

(1) 实验条件

① 由 Pentium Ⅱ以上微机构成的已连网机房。

② DOS、Windows NT(NT Server 或 NT Workstation)及 Windows 98 软件。

③ 网卡驱动程序盘。

④ 分区工具软件。

⑤ 代理服务器软件，如果需要做代理网关的实验，网关机应安装双网卡。

⑥ 接入 Internet 的设备和条件。

⑦ 如果条件许可，应作路由器的设置实验，以方便进行安全策略的实验。

(2) 实验说明

本书的主要目的是设计、建设和管理一个单主域的 NT 网络，安装

NT Server 时应注意不要使用硬盘整体备份等方法，否则“域”的信任关系实验无法实现。

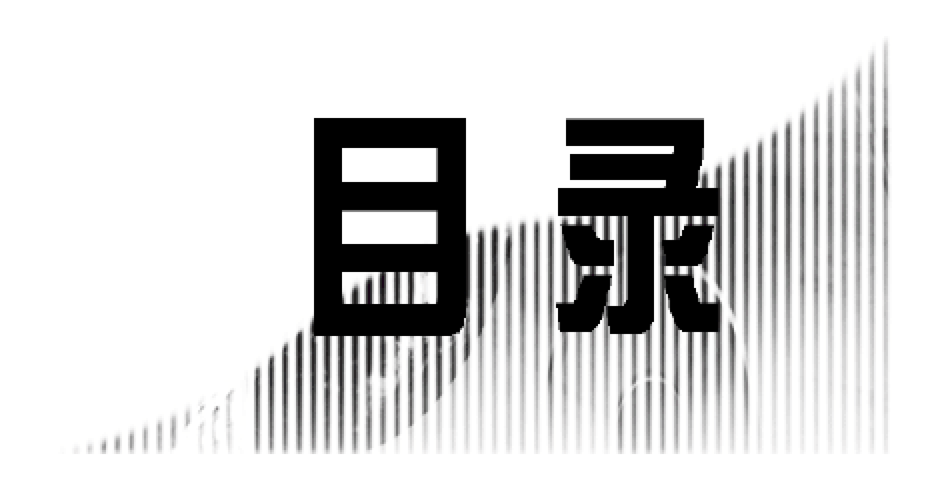
以上只是一个建议性的安排，由于“网络管理”这门课具有很强的操作性和弹性，不同的读者可根据自身的基础选择学习。例如，对于管理和建设小型网络的读者，可以只学习本书第 2 部分的内容；而对于管理和建设中型网络的读者，则可以根据自身的需求，追加部分内容。

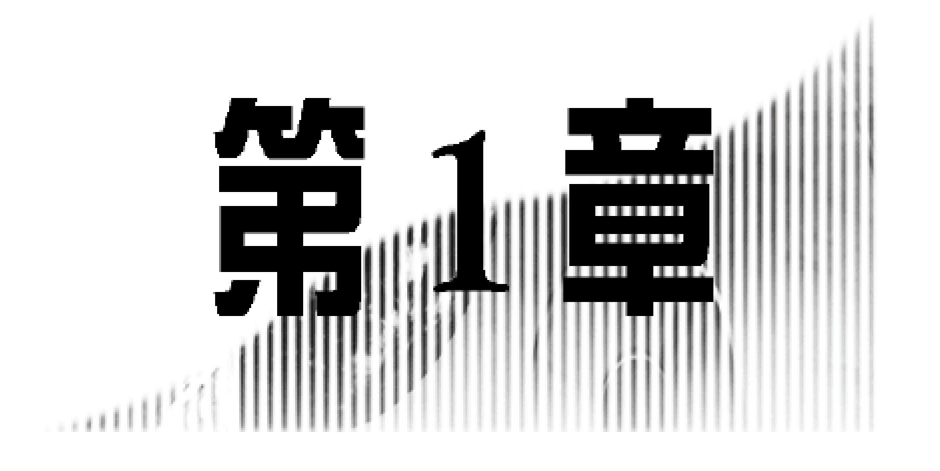
全书由尚晓航副教授主编，同时负责全书各章的主审工作。参加本书创作和编写工作的还有张姝讲师。在本书的编写过程中，得到了北京联合大学陈强教授和孙建华副教授的指导和帮助，还得到了清华大学出版社的大力协助，在此一并表示衷心的感谢。

由于作者学识有限，加上时间仓促，所以书中难免有不妥和错误之处，恳请广大读者批评指正。

作者

2002 年 10 月


目录



第1章 网络管理概论

本章重点介绍网络管理的意义、目标、功能、系统模型、协议和组成等网络管理的基础知识。通过本章的学习，网络管理员应当掌握网络管理的基本概念，并明确网络管理的5个基本标准和功能。

主要内容：

- 网络管理的重要性；
- 网络管理的基本概念；
- SNMP 简单网络管理模型和协议；
- 网络管理系统的基本组成；
- OSI 网络管理的标准和功能。

1.1 网络管理简介

1.1.1 网络管理的意义

网络管理的历史相当久远。自从有了电话交换网，就有了对通信网络的管理，只不过那时的管理技术自动化程度不高。

计算机网络管理技术的发展是与 Internet 的发展同步进行的，随着网络技术的发展，网络规模逐渐增大，复杂性不断增加，异构性越来越高，网络管理技术也得到了迅速的发展。时至今日，计算机网络时代和全球信息化已经到来，网络管理和网络安全性等问题的重要性日益突出。因为，一旦计算机网络崩溃，将会给企业、公司、单位网络中的各种数据和信息资源，以及人们的工作、学习和日常生活带来巨大的损失。因此，网络管理成为网络技术发展中的一项重要技术，它不但对网络技术的发展有着重要的影响，也是现代信息网络中最重要的研究课题之一，并为越来越多的人所重视。从 20 世纪 80 年代起，随着一系列网络管理标准的出台，出现了大量的商用网络管理系统。

随着网络规模的扩大，网络已不再是单一型的网络，而是由若干个大大小小的子网组成，同时集成了多种网络操作系统的平台，包括各种不同厂家、公司的网络设备和产品。此外，为了提供各种网络服务，还集成了多种网络软件。因而，如果没有一个高效的网络

管理系统，则很难向网络用户提供正常的网络服务，也很难保障网络能无故障、安全地运行。因此，为了保证计算机网络中硬件设备和软件的正常运转，除了需要专门的网络管理技术人员之外，还需要利用专用的网络管理工具来维护和管理网络的运行。

总之，现代化的网络管理技术集通信技术、网络技术、Internet 服务技术和信息处理技术等于一身，而现代化网络的管理员则应当能够通过网络管理平台和管理工具调度和协调资源的使用，并可以对网络实行配置管理、故障管理、性能管理和安全管理等多方面管理工作的人员。

1.1.2 网络管理的重要性

为了避免目前存在的重建设、轻管理的现象，网络管理员首先应清楚地认识到网络管理的重要性。随着信息网络的迅猛发展，网络管理的重要性日益突出，其主要原因如下所述。

1. 网络的规模日益增大

目前，Intranet 网络的规模越来越大，企事业单位的一个或多个内部网络通过各种网络互联设备和通信设备等互相连接在一起，并和外部网络 Internet 连接起来。例如：通过网络的连接，可以使打印机、磁盘、传真机和调制解调器能够被多个用户共同使用；远程局域网的用户通过电话线等通信线路就可以远程访问公司总部数据库中的资源。在实际工作中，网络的故障随时可能发生，如果是网络的关键设备发生故障，如网络主服务器崩溃，其带来的损失将是不可估量的。

当管理一个具有 500 个客户机的网络时，必须为每台计算机配置 TCP/IP 协议，还必须对众多的 IP 地址进行日常的管理，这些工作如果靠网络管理员手工完成，将是一项耗时、费力的大工程，而利用动态主机配置协议(DHCP)服务完成上述工作则仅仅需要几分钟的时间。由此可见，对于复杂的大型网络的管理，按照传统的管理方式，仅靠网络管理员进行手工作业是绝对不可行的。现代网络的管理员应尽可能地借助于网络管理工具建立起先进的网络管理系统。

2. 网络资源和网络服务日益丰富

如今计算机网络的应用，已经从早期的简单数据传输发展到了包括语音、图像、视频等多种媒体的信息化网络服务，即从简单数据传输向综合数字业务方面发展。由于网络中的信息资源越来越丰富，因而如何有效地配置、分配、控制和管理网络上的各种类型的资源和服务，已经变得越来越重要，其管理的难度也必然随之增加。此外，由于网络功能与安全的矛盾日益突出，因此，网络管理系统对内网中使用 Internet 的服务以及外网对内网的访问控制管理的安全要求也随之提高。

3. 网络管理日益困难

目前，网络系统的规模正日益扩大，网络的应用水平也随之不断提高，使得网络的维护成为网络管理的重要问题之一。例如，现代化的网络集成了各种设备，各种大型机、小型机、微机、终端、集线器、网桥、路由器和网络交换机等在不断出新，并在此基础上集成了多种软件技术和各种服务技术。这些硬件和软件可能来自于不同的厂家、遵守着不同的标准，使用了不同的技术。因此，对这些网络软件、硬件和信息资源等进行的维护、管理和

故障诊断工作也变得日益困难。对网络故障的排除也变得更加困难，由此导致了维护成本的一路攀升。

4. 网络安全的矛盾日益突出

随着网络的普及，由于计算机病毒、网络黑客、信息间谍等大量出现，对网络安全的威胁日益增加。由此引起的网络安全问题日益突出，并逐步引起人们的警觉。为了防止计算机病毒、网络黑客、信息间谍的入侵，确保网络硬件设备、软件和信息资源的完整性和安全性，人们已经不能只关心网络的功能，而必须越来越多地关注和解决好网络安全方面的问题。

如上所述，信息技术领域的工作正在变得越来越复杂，企业中的任务也变得越来越富有战略性。简单的同种局域网已逐步被取代，今天的网络管理员正面临着一项艰巨而不可避免的任务，这就是管理由各种 LAN、Intranet 和 Extranet 构成的混合信息网络。

1.1.3 网络管理的基本概念

说到网络管理的实施者，自然会联想到网络管理员。实际上，随着计算机网络规模的日益扩大，网络上的设备越来越多。采用传统的人工方式的管理模式来维护和管理日益庞大的现代化网络，显然是非常困难的、不可行的。因而，在现代化网络中，网络管理员必须使用专门用于网络管理的软件，对网络实行自动监测、控制和管理。

为此，网络管理的实施者应该包括网络管理平台和网络管理员两个主体。为了管理好一个网络，网络管理员应当具有如下一些网络管理方面的基本知识。

1. 网络管理(network management)的定义

对于一个网络来说，首先应当建立起网络，实现网络设计的功能。其次，是通过网络管理系统保证建立起的网络系统能够持续、正常、稳定、安全和高效地运行。此外，当网络出现故障时，网络管理系统还应当能够进行及时的报告和处理，从而保障网络的正常运行。因此，网络管理就是为了完成上述目标而对网络系统实施的一系列方法和措施，换言之，网络管理就是指通过某种方式对网络状态进行的调整，其目的是使网络能正常、高效地运行，并使网络中的各种资源得到更加高效的利用，当网络出现故障时，系统应能及时地作出报告和处理。

2. 网络管理的分类

网络管理为控制、协调和监控网络资源提供了手段，其实质就是网络管理者与被管理对象之间如何利用网络实现信息交换，最终完成网络管理的功能。

通常可以将网络管理分为以下两类：

① 狭义网络管理　仅指对网络交通量(traffic)等网络参考性能的管理；

② 广义网络管理　是指对网络应用系统的管理。

3. 网络管理系统

(1) 网络管理系统的定义

通常网络管理是由网络管理系统来实施的，对一个网络管理系统的定义应当包含以下几项内容：

① 系统的功能。一个网络的管理系统首先应明确其具有的功能。

② 明确网络资源。在网络管理中,对于网络资源的管理占有很大一部分比重。网络资源通常被定义为网络系统的软件、硬件及所提供的网络服务和信息等资源。由此,在网络管理系统中只有明确地表示网络资源,才能对它们实施管理。

③ 表明网络的管理信息。网络管理系统对网络实施管理时,必须依赖系统中的网络管理信息,因此,在设计网络管理系统时,必须解决如下问题:

- 如何表示用于网络管理的信息?
- 如何传送上述信息?
- 传送信息中使用何种协议?

④ 确定网络管理信息的结构,即使用什么结构的网络管理系统对网络实现管理。

(2) 网络管理系统的基本功能

一个实用的网络管理系统应当包括以下基本的网络管理功能:

① 为用户制定、设置和实施系统的授权访问策略;

② 为用户制定、设置和实施共享资源的授权访问策略;

③ 能够收集和监控网络中各种设备和设施的工作参数,并能够依据这些信息进行处理、管理和控制。

4. 网络管理的目的和功能

(1) 网络管理的目的

从理论角度看,网络管理集通信技术、网络技术和信息技术于一体,通过调度和协调资源,进行配置管理、故障管理、性能管理、安全维护和计费等管理,达到网络可靠、安全和高效运行的目的。

一般地说,网络管理的目的就是使网络中的各种资源得到有效的利用,保证网络的正常运行。

(2) 网络管理系统的内容和整体功能

从宏观和整体功能来说,网络管理涉及以下 3 个部分的内容:

① 网络服务提供(network service provisioning) 是指向用户提供新的网络服务类型、增加网络设备和提高网络性能等。例如:在局域网内增加 Internet 访问服务时,根据选定的接入服务,选择了路由器作为接入设备,管理员除了需要对路由器和计算机等设备进行设置之外,为了确保网络的安全,可能还需要设置防火墙。

② 网络维护(network maintenance) 是指网络性能的监控、故障报警、故障诊断、故障隔离和故障恢复等。例如,在系统分区容量不足时,系统除了能够记录故障之外,还能向位于本地或远程的管理员主动地发出报警信息。

③ 网络处理(network administrator) 是指网络线路和设备利用率的采集、分析,以及为提高网络利用率所采取的各种控制。

1.2 网络管理系统的组成与功能

在介绍网络管理系统之前,首先需要了解网络管理系统的基本模型,以及网络管理中常用的协议等基础知识。

1.2.1　网络管理系统的基本模型

公认的网络管理系统基本模型由 4 部分组成：即多个被管代理（agent）、至少一个网络管理者或称管理工作站、一种通用的网络管理协议（CMIP 或 SNMP）和一个或多个管理信息库（MIB）。网络设备、计算机主机、应用等被称为被管设备，在这些设备上驻留有代理，代理实际上是一个小巧的应用程序。管理者也是一个程序，负责与用户交互，并通过代理对设备进行管理。管理者与代理通过网络管理协议通信。MIB 相当于一个数据库，提供有关被管网络设备的信息。因此，网络管理系统的模型包含以下 4 个基本的逻辑部分：

① 管理对象　指网络中具体可以操作的参数。

② 管理进程（manager）　指对网络中的设备和设施进行全面管理和控制的软件程序。

③ 管理信息库（MIB）　指记录网络中各种管理对象的信息库。

④ 管理协议（CMIP 或 SNMP）　用于在管理系统与管理对象之间传递和解释操作命令。

下面将介绍 SNMP 简单网络管理模型和协议的有关概念。

1. SNMP 网络管理协议的工作方式和特点

SNMP 是 simple network management protocol 英文单词的缩写，它的中文名称为简单网络管理协议。它是在 1988 年制定出来的，并受到了各厂商的欢迎，现在已经成为事实上的网络管理工业标准。目前，为了便于网络管理软件的使用，在大中型网络中通常要求所购置的网络设备支持 SNMP 协议。

SNMP 协议主要用于 OSI 7 层模型中较低层次的管理，它采用轮询监控的工作方式：管理者按一定的时间间隔向代理请求管理信息，根据管理信息判断是否有异常事件发生；当管理对象发生紧急情况时，也可以使用称为 trap（陷阱）信息的报文主动报告。

SNMP 是为了方便在 TCP/IP 上使用而开发的，但是其检测、控制活动却独立于 TCP/IP，它采用 TCP/IP 协议模型提供的无连接数据报传输服务（UDP）。

SNMP 的优点是协议简单，易于实现；缺点是管理通信开销大。

2. SNMP 网络管理模型

SNMP 模型的体系结构如图 1-1 所示。

（1）管理进程（manager）

管理进程是一个或一组软件程序，它一般运行在网络管理站或网络管理中心的主机上。它在 SNMP 协议支持下命令管理代理执行各种管理操作。管理进程的功能是完成各种网络管理功能，通过各种设备中的管理代理实现对网络内的各种设备、设施和资源的控制。另外，管理人员还可以通过管理进程对全网进行管理。管理进程可以通过图形用户接口，以容易操作的方式显示各种网络信息，以及网络中各网络代理的配置图等。有时，网络进程也会将各个管理代理中的数据集中存储，以备事后分析。

（2）管理代理（agent）

管理代理是一种在被管理的网络设备上运行的软件，负责执行管理进程的管理操作。

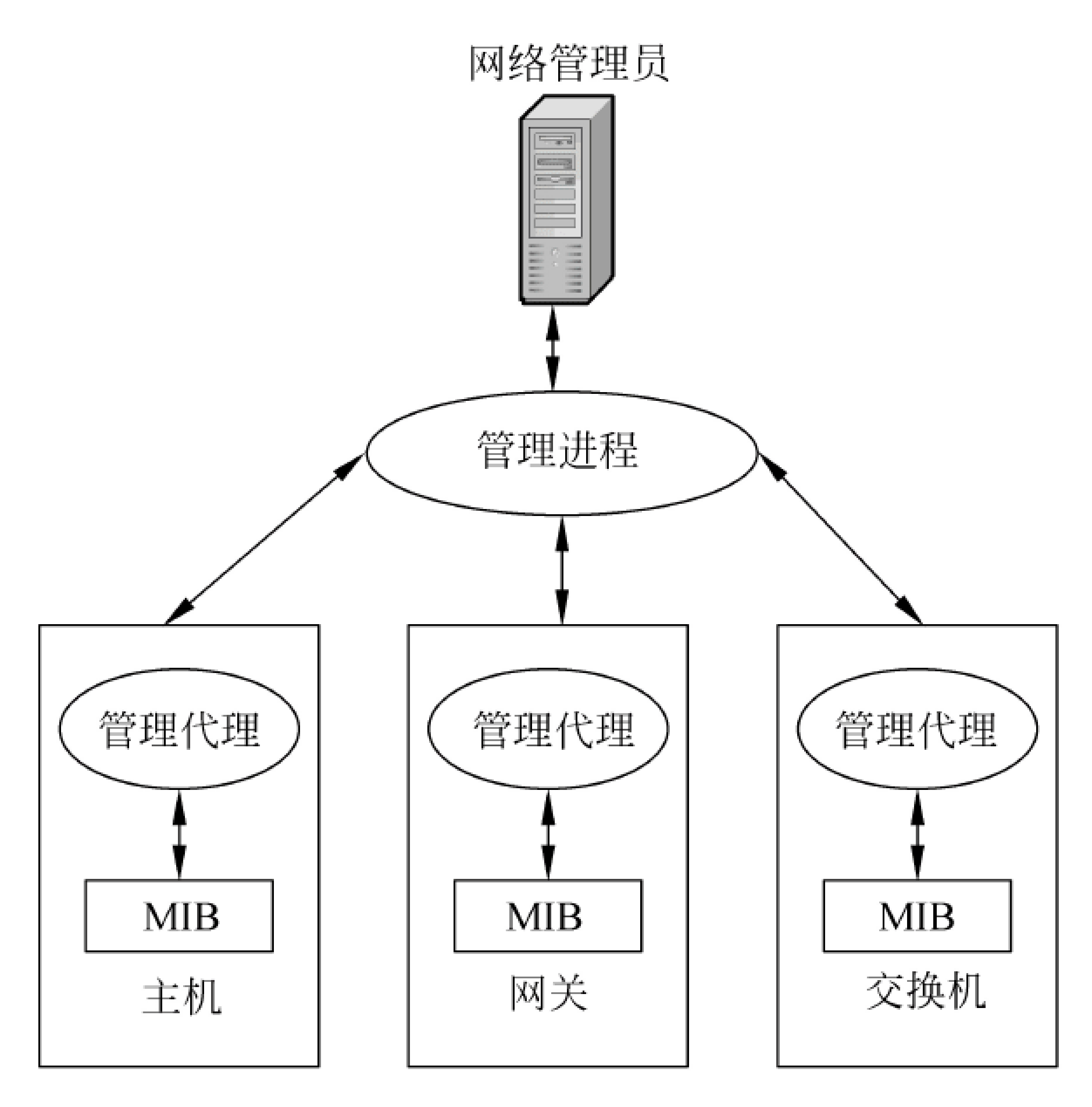


图 1-1　SNMP 网络管理模型的结构

管理代理直接操作本地的信息库 MIB，还可以根据要求改变本地信息库或将数据直接传送给管理进程。管理代理具有两个基本的管理功能：

① 读取 MIB 中各种变量的值，这里的变量就是管理对象；

② 修改 MIB 中各种变量的值。

(3) 管理信息库(MIB)

MIB 管理信息库记录管理对象的各种信息。它是一个概念上的数据库，由各个管理对象组成，每个管理代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

(4) 管理协议

用于在管理系统与管理对象之间传递和解释管理操作命令的 SNMP 协议。许多网络管理软件要求所管理的设备支持 SNMP 协议，如果不支持，则无法使用该软件实现对网络系统设备的自动识别和管理功能。如 HP 公司的 Open View 软件。

1.2.2　实际网络管理系统的组成

介绍了网络管理的各种人为因素和网络系统管理的基本模型之后，本小节开始讨论网络管理系统的实际组成和工作状况。实际的网络管理系统的组成如图 1-2 所示，由 4 个基本部分组成，即管理软件、管理代理、管理信息库和代理设备。

在大部分的实际网络管理系统中，只有前 3 个部分，因此这 3 个部分是基本和必需的，而并非所有的网络都有“代理设备”，因此，第 4 个部分是可选的。下面将分别介绍这几个基本部分的功能和工作联系。

1. 网络管理软件

网络管理软件简称“网管软件”，它是协助网络管理员对整个网络或网络中的设备进行日常管理工作的软件。网络管理软件除了要求网络设备的“管理代理”定期采集用于管

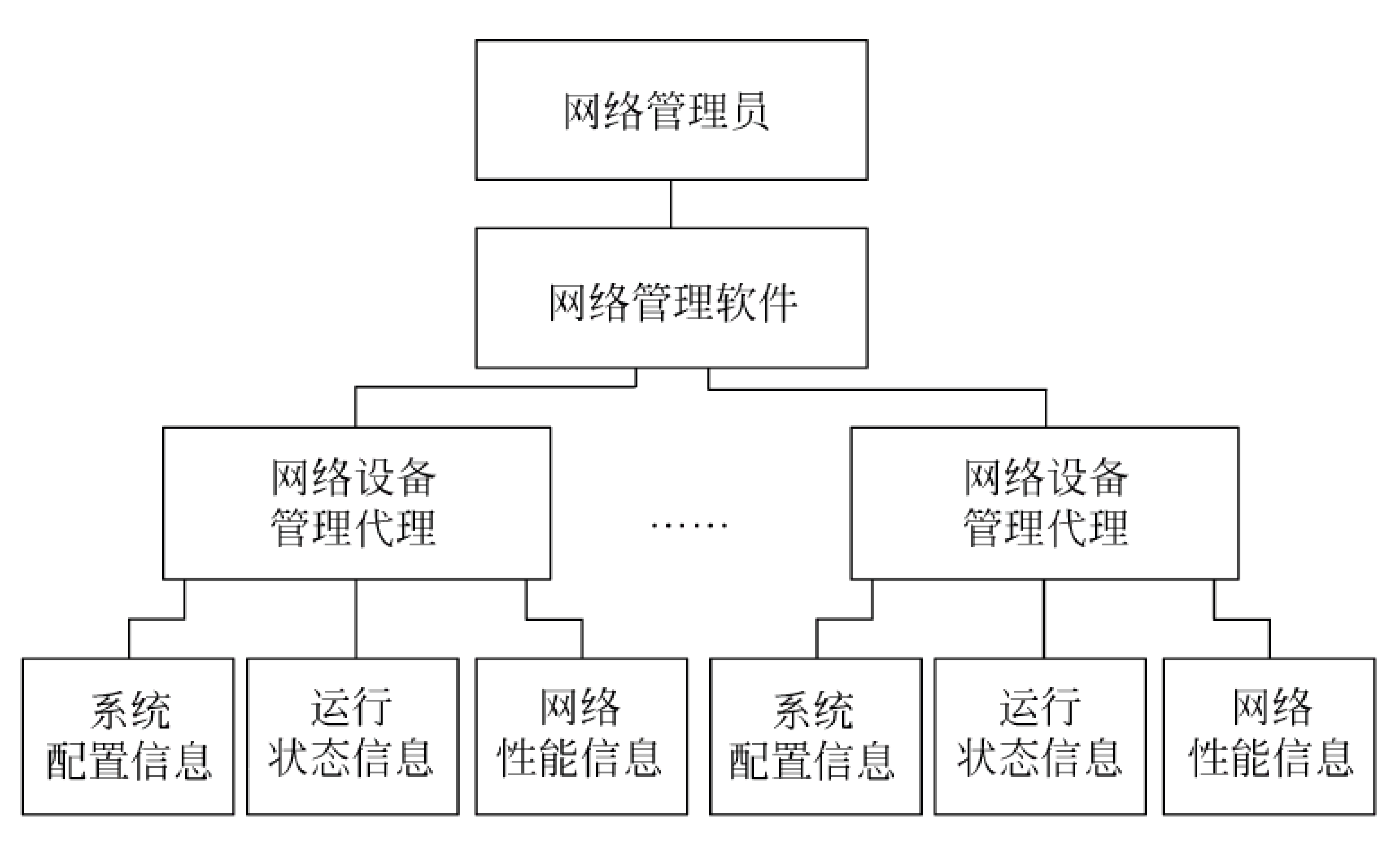


图 1-2　网络管理系统的组成结构图

理的各种信息之外,还要定期查询管理代理采集到的主机有关信息,如系统配置信息、运行状态信息和网络性能信息等。网管软件正是利用这些信息来确定和判断整个网络、网络中的独立设备或者局部网络的运行状态是否正常。

在网络管理系统中,网络管理软件是连接其他几个因素的桥梁,因此有着举足轻重的地位。它的功能的好坏将直接影响到整个网络管理系统的功能。

对于大型网络来说,网络规模较大,网络结构复杂,一旦网络出现故障,查找与维护都很困难,因此,网络管理软件是不可缺少的助手;而对于小型网络或个人用户来说,他们的技术水平较低,聘请专业技术人员的费用又太高,因此网络管理软件可以帮助解决一些棘手的问题。由此可见,网络管理软件已经成为各种网络中必不可少的组成部分。

市场上的网络管理软件名目繁多,因此选择网管软件已成为很多用户关心的问题。选择时可以从以下几方面进行考虑:与自身的管理规模和网络模式(如 C/S)相应;具有智能化的监视能力;具有基于用户策略的控制能力;具有支持多协议、开放式操作系统和第三方管理软件的能力;具有良好的用户界面;具备简单的、无需编程的开发工具;具有良好的技术支持和服务;合适的性能价格比。

2. 网络设备的管理代理

网络设备的管理代理简称"管理代理",它是驻留在网络设备中的一个软件模块。其中的网络设备可以是系统中的网络计算机、网络打印设备和交换机等。网络设备的管理代理软件能够获得每个网络设备的各种信息,如设备运行状况、系统配置、设备特性和性能等信息。因此,每个管理代理上的软件就像被管理设备的代理人,它可以完成网管软件所布置的信息采集任务。实际上,它充当了网络管理系统与被管理设备之间的信息中介。管理代理通过被控制设备中的管理信息库(MIB)来实现管理网络设备的功能。

在实际应用中,由于 SNMP 协议确立了不同设备、软件和系统之间通信的基础框架。因此,人们通常选用支持 SNMP 协议的网络设备,如选择支持 SNMP 协议的服务器、路由器、交换机和集线器等。这样驻留在其中的管理代理软件就具有了共同语言。正因为有了这个标准语言,网络设备的管理代理软件才可以将网络管理员软件发出的命令按照统一的网络格式进行转化,再收集需要的信息,最后返回正确的响应信息,从而实现了网

管软件在网络管理系统中的统一网络管理。

3. 管理信息库

如前所述，管理信息库(MIB)定义了一种有关对象的数据库，它由网络管理系统所控制。如图 1-1 所示，整个 MIB 中存储了多个(可多达上千个)对象的各种信息数据。网管软件(在 SNMP 模型中又称管理进程)正是通过控制每个对象的 MIB 来实现对该网络设备的配置、控制和监视的。而网络管理员使用的网络管理系统可以通过网络管理的代理软件(管理代理)来控制每个 MIB 对象。

4. 代理设备

在网络管理系统中，代理设备是标准的网络协议软件和不支持标准协议的软件之间的一座桥梁。利用代理设备，无需升级整个网络管理系统即可实现旧版本网管软件到新版本的升级。例如，某网络正在使用的是支持旧版本 SNMP 协议的网管软件，当新版本 SNMP 协议开发出来之后，如果直接升级，则整个网络中所有的现存设备都会受到影响，使用代理设备则可以方便地解决此类问题。注意，正是由于代理设备的上述特殊功能，所以不是所有的网络管理系统中都有这种设备，也就是说，代理设备在网络管理系统中是可选的。

5. 网络管理系统设计时的准则

在设计和构造网络管理系统的结构时，必须遵循以下几条网络管理的基本准则：

① 不应当由于网络管理信息的增加而导致网络通信量的明显增加。

② 不应当由于被管理设备上协议代理的存在，而增加系统处理的额外开销，以致影响到该设备的主要功能的实现。

③ 网络管理员应当遵循国家颁布的各种网络管理的法规。

1.2.3 网络管理的标准和主要功能

在对网络管理和网络管理系统有了比较全面的认识之后，就需要了解网络管理的主要功能。国际标准化组织(ISO)从较大规模网络的管理应用实际出发，在 ISO/IEC 7498-4 文档中定义了网络管理的 5 大功能，这些功能被广泛接受和认可。这 5 大功能是：网络的故障管理、网络的配置管理、网络的计费管理、网络的性能管理和网络的安全管理。

本节将对这 5 大功能进行详细的介绍。

OSI 网络管理标准制定的宗旨：首先，是为了满足不同网络管理系统之间进行相互操作的需要；其次，是为了满足各种网络互联设备在网络管理方面的需求。

1. 网络的故障管理(fault management)

网络的故障管理也称失效管理，其主要任务是自动地检测和记录网络的故障，并及时通知给网络用户，以使网络能够正常有效地运行。网络中的差错故障等可以导致网络系统的瘫痪或网络性能下降到不可接受的地步，因此，网络中的故障管理是网络中可以实现的最为广泛的一种管理，它是网络管理的基本功能之一。

(1) 网络故障产生的原因

故障是指一个系统在外界异常因素的作用下，引起的系统功能和性能明显下降的现象。计算机网络系统是由多个节点和各种通信设备互联而成的，因此，计算机网络系统的

故障主要来源于各计算机节点的故障和通信信道本身的故障。例如，电磁的干扰、环境温度过高、环境湿度过大、环境尘埃过多、电源电压波动幅度过大等均可引起网络故障。

(2) 故障管理系统的功能

当了解到网络故障出现的主要原因之后，就可以针对故障产生的原因进行解决，这就是网络故障管理应当完成的任务。故障管理的目的在于保证网络的正常连接、并能够提供有效的网络服务。因此，网络故障管理的功能应当包括以下几个方面：

① 能够检测或接收到管理对象发生的故障及其产生的故障报警；

② 能够使用冗余的网络对象替代故障对象来提供临时的网络服务，例如，在NT/Windows 2000 中使用备份域控制器替代主域控制器来提供身份验证的服务；

③ 能够自动创建和维护故障日志的信息记录库，并对故障日志进行分析，例如，NT/Windows 2000 中的系统警报功能；

④ 可以进行故障的诊断并能追踪故障，确定故障的性质及故障的解决方案；

⑤ 能够排除故障，恢复正常的网络服务。

例如：网络中有一个名为 WL01 的用户节点，它与主干网之间仅有一处连接，假定某日发生了故障。在该网络中，网络管理系统的作用是：第一，收集信息发现故障，即可以告诉用户有故障发生了，用户将不能通过 WL01 节点访问网络；第二，决定哪些管理失效了，即管理工具应该有能力分析出引起该故障的原因，例如经分析得出结论是该节点与主干网的串行连接出现了故障；第三，失效的提示和解决，如管理工具应提示用户排除这个连接故障。通过这个例子可以看到，适当地使用故障管理可以提高故障的排除效率，使得用户不致停机过长，当然，这要取决于网络管理工具智能化的程度。

(3) 故障管理系统的组成

故障管理系统通常包括以下几个基本功能模块：

① 故障检测　检测管理对象的差错现象，或接收管理对象的差错事件通报，以确定故障位置和性质。

② 故障诊断　进行诊断测试，以跟踪并确定故障位置与故障性质。通过故障诊断找出发生故障的原因和解决办法。

说明：对网络故障的诊断和检测主要是依据网络组件的状态检测情况来确定的。不严重的简单故障可以通过错误日志的记录信息而确定，通常不做特别处理。对于严重的故障，则需要通过网络管理器的“报警”功能实现诊断和处理，一般情况下，网络管理器可以根据相关的信息对报警进行处理和排除。当网络故障更为复杂时，网络管理器可以通过执行诊断和测试程序来辨别故障原因。

③ 故障恢复　不仅包括故障排除，还包括如何避免故障的发生，及减少故障发生的措施。

(4) 故障管理工具的选择

当用户确定了需要处理和管理的故障类型之后，就需要选择合适的故障管理工具。应当根据网络管理的需求和具体环境来选择适宜的故障管理工具。按照故障管理工具的复杂程度可进行如下的分类：

① 简单的故障管理工具　最简单的工具可以确定故障的存在，但不能指明故障发生的原因。例如，在TCP/IP网络中，使用ping命令向网络上的设备（每一个主机和节点设备）发送ICMP（Internet控制报文协议）信息包，以判断IP网络层的连通性好坏。

② 复杂的故障管理工具　倘若网络上的主机和设备较为复杂，并且具有报告网络事件的能力，则应当开发或选择一种复杂的故障管理工具，该工具可以利用主机、节点设备的内在能力。这样，当这个故障管理工具通过记录的事件，或查询的方法检测到故障的时候，它就会及时通告网络中的失效状况。

③ 高级的故障管理工具　上述复杂的故障管理工具只完成了故障管理中的大部分工作，但是没有完成"排除故障"的功能，而高级故障管理工具应当具有这种能力。计算机网络中的许多失效现象都是由网络设备的故障而引发的，但故障并不总是出现在硬件上。例如，网络上有可能出现两个系统不能正常进行电子邮件通信的现象，如用户shang在主机A上给主机B上的用户guo发送的所有电子邮件均未成功。而此时，故障管理工具显示每个网络设备都是可用的，也没有出现设备发送的故障事件报告，但故障的存在是显而易见的。高级故障管理工具可以通过更加复杂的故障检测、跟踪的方法最终分析判断出故障的来源，并能够排除这个故障。例如高级故障管理工具会判断出本例中的某个集线器的端口在传递大的数据包时会出现超时的故障，并由此导致了通信的失效，经处理后，管理工具排除了这个故障。

2. 网络的配置管理（configuration management）

网络的配置管理是指发现和设置网络上关键设备的过程，其目标是为了实现特定的网络功能，或者是使网络的性能达到最优。在日常管理中，配置管理是实现网络各种功能的起点，它用于配置网络，同时也可以优化网络。配置管理在日常网络管理中有关的任务和功能叙述如下：

（1）网络配置管理的基本任务

① 发现网络设备的配置管理　发现网络设备的清单和位置的工作一般由网络中的拓扑自动发现模型完成，当然也可以由管理人员添加和删除管理对象。网络管理员必须掌握和控制互联网络的状态，包括网络内各种设备的状态及其连接关系。例如，在社区宽带网中，可以安装网管软件，自动监控网络上的在线工作节点。

② 网络设备的配置管理　即设置网络关键设备的参数、服务和连接，使它们能够完成预期的任务。例如，在新组建的网络中，完成网络中各设备的功能、设备之间的连接关系和工作参数的配置。

（2）配置管理系统的基本功能

为了辨别、定义、控制和监视一个网络对象，配置管理必须具有下述功能：

① 识别被管网络的拓扑结构；

② 监视网络设备的运行状态和参数；

③ 自动修改指定设备配置；

④ 动态维护网络。

（3）配置管理的工具

配置管理工具一般可以自动收集和更新网络设备的数据，并能够生成网络设备的清

单及其他报告，如配置报告等。根据工具的复杂程度、功能的不同，配置管理工具也可以分成简单、复杂和高级等几种类型。

① 简单的配置管理工具应当能够提供网络信息的中心存储功能，例如，网络信息应当包括：网络地址的分配、序列号、物理位置和设备的其他固定信息等；此外，它还能为用户提供一些便于查找和搜索信息的功能。

② 复杂的配置管理工具应当具有更高的功能。例如，它能够自动收集和存储所有网络设备的信息，提供系统当前配置与在系统中存储的配置的比较功能，此外，还可以提供远程配置设备运行参数的功能等。

③ 高级的配置管理工具是用关系数据库管理系统（RDBMS）对外部网络信息进行存储、关联、查询的，它可以建立设备的清单，并具有更高的效率，此外，它还能够对设置和配置进行评价。

3. 网络的计费管理（accounting management）

（1）计费管理的目标

计费管理用于记录网络资源的使用情况，其目的在于控制和监测网络操作的费用和代价。它对于公共商业性网络是不可缺少的部分，网络管理员可以通过“计费管理”软件规定用户可以使用的最大费用，以控制用户占用过多的网络资源。这样，可以从另一个角度提高网络的效率。

（2）计费管理的基本功能

计费管理的主要功能包括：维护用户基本信息、输入计费的策略、统计出网络通信资源和信息资源的使用情况、分析预测网络业务量等。例如，可以根据用户的基本信息和计费策略计算出用户的账单，向用户提供计费信息查询，以及控制用户使用的最大费用和资源等。

计费管理可分为以下 4 个基本功能模块：

① 服务事件监测　该模块从管理信息流中，过滤出用户使用网络服务的有关事件，自动记录和统计用户使用网络资源的情况。例如，根据采集的拨号数据统计通信线路的使用次数、传送的信息量等，并把这些事件存储到用户账目中，以供用户查询，最后还要把这些信息送到资费过滤模块，用于核算和统计费用。

② 资费管理服务　该模块根据资费标准计算出使用费用。例如，根据资费策略和预先规定的用户费率对用户使用的网络服务进行费用核算。

③ 服务管理功能　该功能是指对用户的可选路由和可以获得的服务进行设置和限定。例如，对于有些用户，在每日的固定时间段内，限制其使用大容量的传输业务。又例如，对在某个时间段使用网络资源的用户提供折扣优惠等。

④ 记账控制功能　记账控制功能支持网络操作人员输入的账号、费率调整数据以及其设置的服务规则等操作。

对于公共商业性网络来说，计费管理是最重要和最麻烦的任务。计费管理通常使用某个附加的管理软件来实现。如“美萍网络管理大师”是常用的网吧计费管理的软件。

4. 网络的性能管理（performance management）

网络性能管理的主要内容是考察网络和网络中各个对象的利用率和性能，以验证网

络服务是否达到了预期的水平，同时还应该能够找出网络现有的和潜在的瓶颈，并实施相应的调整措施。

（1）性能管理的两个基本目标

① 保证网络应用服务的高质量、高性能和高可用性等，例如差错性能、快速响应性能等。

② 保证系统资源的合理利用，例如信道的利用率、主机中 CPU 的利用率和磁盘空间的利用率等。

上述两个方面是密切相关的，不可偏废。例如，当系统资源经常处于紧张状态时，虽然资源的利用率很高，但是却会影响到系统应用服务的质量和性能；反之，如果资源的利用率较低，则系统应用服务的质量就会较高，然而，由于系统资源经常处于闲置的状态，因此也不能算作是一个好的系统。

综上所述，网络性能管理的最终目标就是通过对系统有关性能参数的实时监控、调整和优化管理，使系统不仅有较高的应用服务质量，也能有合理的系统资源利用率。

（2）性能管理的基本功能

性能管理包括一系列的管理功能，其基本功能应当包括以下几个方面：

① 收集和统计被管理对象的各种性能参数，例如网络性能数据和历史数据等。

② 对当前数据进行统计分析，检测性能故障，产生性能报警，并报告与性能有关的事件。

③ 在当前数据的统计和分析基础上，与历史模型进行比较后，做出趋势预测。

④ 形成和改进网络性能评价的规则和模型。以性能管理为目标，进一步改进网络的操作模式。

总之，性能管理就是通过监控网络的运行状态，调整网络性能的参数来改善网络性能，确保网络平稳运行。性能管理对系统的运行和通信效率等系统性能进行评价和分析，其分析结果可能会触发某个诊断和测试过程，进而可能导致网络的重新配置，以维护这个网络的性能，并维持和分析性能日志。

5. 网络的安全管理（security management）

（1）安全管理的目标

网络安全管理的目标是保证网络不被非法使用和破坏，保证网络管理系统的安全，并防止用户资源的非法访问，确保网络资源和网络用户的安全。

（2）安全管理的基本功能

针对网络中常见的安全问题，如网络数据的安全性、网络的授权许可和网络资源的访问控制等，网络安全管理应当包括以下几项基本的内容：

① 身份验证　保证只有合法的用户才能登录和访问到许可访问的网络资源。

② 密钥管理　包括密钥的生成、分发和控制，以及密钥安全的控制措施等，如密钥的分发与其访问权限的设置。

③ 安全控制　包括生成和维护访问控制数据库，分析并发出与安全有关事件的通知，记录、维护和浏览安全日志，以便对安全问题进行事后分析。例如，当银行网络资源的所有者的控制权限被网络管理人员剥夺，或者是黑客企图通过“穷举法”破译口令时的安

全日志会对日后的分析和跟踪起到重大的帮助作用。又如,当网络被非法入侵或非授权用户访问时,发出特定的警告和提示信息等。

④ 访问控制　包括创建、启动、控制和终止各种与网络安全有关的服务和设施。

总之,网络安全管理的主要目标应该是确保网络资源的安全。因此,安全管理的主要内容是对网络资源和信息访问进行约束和控制,包括验证和控制网络用户的访问权限和优先级,同时还应检测和记录未经授权的用户对网络实施的非正常企图和操作。

除了上述 OSI 的 5 个管理功能域外,随着综合信息系统的广泛应用,网络管理系统还应具有网络规划、网络的信息管理和网络的人员管理等内容。例如,由于 B/S(浏览器/服务器)网络模型的大量使用,用户通过计算机工作站的浏览器,可以沿着信息的超链接和超媒体处的链接搜索信息,因此,要求网络信息管理系统具有对所提供信息内容的不断追踪能力,并确保信息的完整性和可靠性。

由于网络管理集通信技术、网络技术、安全技术和信息技术于一体,因此,涉及的面广,使用时的概念多、技术复杂。归纳起来,网络管理的理论重点和难点为以下 4 点,希望网络管理员在学习中很好地掌握和理解。

- 网络管理相关的基本概念;
- SNMP 网络模型的 4 个组成部分;
- 网络管理系统的基本组成;
- OSI 网络管理标准的 5 个基本内容。

习题

(1) 为什么说网络管理的重要性日益增加?

(2) 什么是网络管理? 它的主要内容有哪些?

(3) 网络管理系统是如何定义的?

(4) 网络管理的目的是什么? 网络管理系统定义了哪些内容?

(5) 网络管理系统的基本模型是什么? 由几部分组成? 每部分的内容又是什么?

(6) 为什么要建立 OSI 网络管理标准?

(7) OSI 网络管理标准的 5 个管理功能是什么?

(8) 网络管理要解决的首要问题是什么?

(9) SNMP 简单网络管理模型是什么? 它由几部分组成? SNMP 协议的特点是什么?

(10) 在什么场合需要购置有网管功能的设备? 这些设备通常支持什么协议?

(11) 网络管理的实质是什么?

(12) 网络管理可分为几类?

(13) 网络管理系统中使用的管理协议的名称是什么? 它有什么作用?

(14) 网络管理的理论重点和难点有哪些?

(15) 网络管理系统设计时应遵循哪些准则?



第2章 网络的接入与互联技术

本章将介绍典型局域网之间通过广域网的互联，以及局域网通过广域网接入Internet时所使用的技术，包括：网络互联设备、可申请的广域网通信服务、广域网的组网技术，以及局域网通过广域网接入Internet的技术等内容。这些知识都是有关设计、组建和管理远程网络的实用知识和基本技术，所以应加强学习，力求真正理解和熟练掌握。

主要内容：

- 网络互联概述；
- 广域网互联技术；
- 申请广域网的通信服务；
- 局域网通过广域网接入Internet的概念；
- 普通用户、小型单位用户的接入技术；
- 大公司及企事业单位用户的接入技术；
- 网络互联范例。

2.1 广域网技术概述

1. WAN的定义

WAN是广域网(wide area network)的英文缩写，WAN定义为使用本地和国际电话公司或公用数据网络，将分布在不同国家、地域甚至全球范围内的各种局域网、计算机、终端等设备，通过互联技术而形成的大型计算机通信网络。

2. WAN的类型与分布范围

(1) WAN的类型

常见的WAN从应用性质上可以划分为以下两种：

① 第一种广域网　是指电信部门提供的电话网或者是数据网络，例如PSTN(公用电话网)、X.25(公用分组交换网)、DDN(公用数字数据网)、FR(公用帧中继网)和宽带综合业务数字网等公用通信网。这些网络可以向用户提供世界范围的数据通信服务。

② 第二种广域网　是指将分布在同一城市、同一国家、同一洲，甚至几个洲的局域

网，通过电信部门的公用通信网络进行互联而成的专有广域网。这类广域网的通信子网和资源子网分属于不同的机构，如通信子网属于电信部门，资源子网属于专有部门。例如，像 IBM、SUN、DEC 等一些大的跨国公司，都建立了自己的广域网，它们都是通过电信部门的公用通信网来连接分布在世界各地的子公司的。

(2) WAN 的分布距离

WAN 的分布距离是指包括 WAN 中的所有主机与工作站点的物理设备分布的地理范围，一般为方圆 10 公里、100 公里或 1 000 公里以上的数量级。

3. WAN 的连接介质

WAN 中的微机工作站和局域网可以使用各种连接介质进行连接。例如，可以通过电话线、卫星、微波、直接数字同步线(DDS)等各种线路进行连接。

4. 常用的广域网协议

(1) WAN 常用的物理层协议

- EIA(electronic industries association，电子工业联合会)定义的串行通信接口标准：RS-232C、RS-422 和 RS-485 等。
- CCITT(international telephone and telegraph consultative committee，国际电话与电报顾问委员会)推荐的 DCE-DTE 接口标准：X.20、X.21 等，分组交换网接口标准：X.3、X.28 和 X.29 等。

(2) WAN 常用的数据链路层协议

- IBM 公司早期推出的 BISYNC 字符控制协议，以及他后来推出的同步数据链路控制协议(SDLC)。
- DEC 公司 20 世纪 70 年代中期推出的 DDCMP 字符计数协议。
- 国际标准化组织(ISO)制定的高级数据链路控制协议(HDLC)。

(3) WAN 常用的网络层协议

常用的广域网网络层协议有 CCITT 的 X.25 和 TCP/IP 协议中的 IP 协议等。

2.2　网络互联的概念

随着社会对网络技术需求的不断增长，以及人们对网络资源使用需求的日益增加，网络互联技术越来越为人们所重视。在网络的实际应用过程中，网络互联技术正在发生着根本的改变，并成为当前网络技术研究中一个新的热点。

1. 网络互联的定义

网络互联的定义是指将分布在不同地理位置的网络、设备相连接，以构成更大规模的网络，并实现更大范围内的资源共享。互联的网络和设备可以是同种类型的网络，也可以是完全不同的网络。例如，国家的信息高速公路就是将不同地区、不同行业、不同类型的网络连接而成的互联网络。对于网络客户来说，互联后的网络对他们应当是透明的，即互联的网络应当屏蔽掉所连接网络在网络协议、服务类型和网络管理方面的差异。

2. 网络互联的功能

网络的互联功能可以分为以下两种基本类型：

① 基本功能　是指互联网络能够提供不同网络之间传送数据的功能。显然基本互联功能应当包括寻址和路由选择功能。

② 扩展功能　是指互联网络能够提供不同服务类型网络互联时应当具备的功能，例如，当互联网络的分组长度不同、协议不同时，应具有处理和转换这些不同的功能。

3. 网络互联的类型

(1) 局域网互联

① 多个近程局域网的互联：其中又包括同种局域网的互联和异种局域网的互联。例如，使用中继器、集线器等设备可以连接多个以太网；使用网桥和交换机可以实现一个以太网和一个令牌环网的连接。

② 局域网通过公用广域网互联为广域网：多个远程局域网可以通过公用的广域网服务进行互联，并形成专有的广域网。一般使用路由器和网关通过广域网 ISDN、DDN 和 X.25 等实现互联，从而形成专有广域网。国内这样的网络有很多，例如，海关总署的骨干网就是这种典型的企业广域网。

(2) 接入 Internet

在网络应用中接入 Internet 的方式主要有以下两种：

① 个人计算机或小型局域网通过电话网接入 Internet，例如，个人计算机、小型公司网络使用普通方式(电话线＋modem＋软件)接入 Internet。

② 局域网通过广域网的服务接入 Internet，例如，使用路由器和网关通过 FR(帧中继)、DDN(数字数据网)和 X.25(分组交换网)等广域网接入 Internet。

2.3　广域网提供的通信服务

在构建互联网络时，首先考虑的就是广域网的连接方式，也就是可以向电信部门或者是 ISP(因特网服务提供商)申请到的公用广域网通信服务。

邮电部门或 ISP 可提供的常用通信服务有以下几种：

(1) PSTN(public switching telephone network)

PSTN 为公用电话交换网，提供通过电话网的计算机通信服务，采用拨号呼叫方式。使用公用电话网进行远程通信时，数据传输速率较低，最高速率为 56Kb/s。它是以时间和距离计费的，因此，费用较高。在公用数据网出现之前，它是远程数据通信的惟一传输途径。

(2) CHINAPAC(X.25)

CHINAPAC 为公用分组交换网，提供数据报和虚电路两类服务，可提供比普通电话线高的信道容量和可靠性。它是最常用的一种广域网资源，目前已连接了县以上的城市和地区。城市间的最高传输速率为 64Kb/s～256Kb/s，而用户的数据传输速率为 2.4Kb/s、4.8Kb/s 和 9.6Kb/s。

(3) ISDN(integrated service digital network)

ISDN 的中文名称是综合业务数字网，俗称“一线通”，它采用数字传输和数字交换技

术，将电话、传真、数据、图像等多种业务综合在一个统一的数字网络中进行传输和处理。它可以为用户提供包括电话、传真、可视图文及数据通信等的经济有效的数字化综合服务。

传统的调制解调器传输的是模拟信号，所以需要有一个“调制”和“解调”的过程，而 ISDN 的传输则是纯数字的过程，因此，通信质量大大提高，经测试表明 ISDN 数据传输比特误码性能比传统电话线路改善了至少 10 倍，此外它的连接速度非常快，通常只有几秒钟就可以拨通。因此，ISDN 从技术角度看是较好的，但是由于它的收费制度没有摆脱电话的占用费用，更没有采取合理的包月使用制度，因此和现在新兴的 ADSL 和 cable modem 相比不仅速度没有了优势，在价格上更不占上风。

- ISDN 的基本速率接口(BRI)：可为用户提供 2 个 B 通道，一个 D 通道。其中一个 B 通道的数据传输速率为 64Kb/s，用来传递数据；D 通道一般用来传递控制信号，其传输速率为 16Kb/s。因此，普通的 ISDN 线路提供的最高数据传输速率为 128Kb/s，当 D 通道也用来传递数据时，BRI 的最高传输速率可达 144Kb/s。
- ISDN 的基群速率接口(PRI)：在不同地区和国家，PRI 提供的总的传输速率有所不同。例如，在北美和日本的 PRI 提供 23B＋D 的数据通信服务，最高的数据传输速率为 1.544Mb/s；而欧洲、中国与澳大利亚等地区，向用户提供 30B＋D 的数据通信服务，最高的数据传输速率为 2.048Mb/s。目前，对于集团客户来说，这也是电信部门所能提供的具有较高速率、较高带宽的一种通信服务，具有较好的性能价格比。

(4) DDN(digital data network)

DDN 为数字数据网，而 CHINADDN 特指中国数字数据网。DDN 是随着数据通信业务的发展而迅速发展起来的一种新型网络。DDN 主干网的传输媒介有光纤、数字微波、卫星信道等，而用户端的传输介质多采用普通电缆和双绞线。DDN 利用数字信道传输数据信号，这与传统的模拟信道相比有着本质的区别。DDN 传输的数据具有质量高、速度快、网络时延小等一系列的优点，特别适合于计算机主机之间、局域网之间、计算机主机与远程终端之间的大容量、多媒体、中高速通信的传输，DDN 可以说是我国的中高速信息国道。

DDN 通常可以向用户提供专线电路、帧中继、语音、传真及虚拟专用网等业务服务，工作方式均为同步。目前，DDN 网络的干线传输速率为 2.048Mb/s～33Mb/s，最高可达 150Mb/s。向用户提供的数据通信业务分为低速(50Kb/s～19.2Kb/s)和高速两种，例如，北京用户可以根据通信速率的需要在 N×64Kb/s(N＝1～32)之间进行选择，当然速度越快租用费用也就越高。例如，在中国电信申请一条 128Kb/s 的区内 DDN 专线，月租费大约为 2 000 元。

DDN 作为一种特殊的接入方式有它自身的优势和特点，也有其特定的目标群体，它较 ISDN 有速率高、传输质量好、信息量大的优点，而相对于卫星通信又有时延小、受外界影响小的优势，所以它是集团客户和对传输质量要求较高、信息量较大的客户的最佳选择。

(5) xDSL

DSL(digital subscriber line)表示数字用户环路,以铜质电话双绞线为传输介质的点对点传输技术。它使软件技术与电子技术有效地结合,充分利用了在电话线路中未被利用的高频部分来传递数据。xDSL 中的“x”可以是 A、H、S、I、V 等,它们分别表示了不同的数据调制技术。目前,xDSL 技术发展非常迅速,其主要原因在于它的低投入,即可以充分利用已有的电话通信线路,不必重新布线和改变基础设施。因此,xDSL 广泛地应用于宽带数据传输业务服务,例如个人微机高速上网、局域网高速接入 Internet、小型网络的远程访问、远程教学,以及视频点播等场合。目前,接入 Internet 时主要采用 modem 的接入方式。例如,SDSL 的最高数据速率为 2.048 Mb/s。

(6) VSAT(very small aperture satellite)

VSAT 表示“超小口径卫星终端”,即各个地球站终端通过静止的通信卫星,与主站一起构成卫星通信网。卫星通信网的用户需要在单位或驻地建立起 VSAT 站(终端),以便通过卫星进行数据通信。VSAT 适用于通信线路架设困难的场合,它容易受气候的影响,也不易在城市应用,其费用较高。

2.4 网络接入技术

2.4.1 网络接入技术概述

随着网络的迅速普及,愈来愈多的 LAN 之间需要互联,并与因特网连接。因此,现代广域网技术的核心就是 Internet 的网络接入技术。

1. 网络接入技术及其基本要求

(1) 网络接入技术

网络接入技术是指一个局域网与 Internet 相互连接的技术,或者是两个远程 LAN 与 LAN 间相互连接的技术。这里所指的“接入”,是指用户利用电话线或数据专线等方式,将个人或单位的计算机系统与 Internet 连接,进而使用其中的资源;或者是使用电话线或数据专线连接两个或多个局域网,实现远程访问或通信。注意,有时网络接入常常专指“宽带接入”技术。综上所述,网络接入技术的实质就是网络互联技术。

(2) 在网络接入技术中应考虑的因素

① 带宽或速率的要求,可以指定上行和下行方向不同速率的带宽或速率。

② 按需连接或永久连接。当采用前者时,可以即连即用,需要上网时即可连入 Internet。而采用后者时,用户可以得到专有的、永久性的连接。

③ 投资和运行费用合理、适宜。

④ 可靠性较高,必要时设计双重接入通道,例如,一个主通道(高带宽),一个备用通道(低带宽)等。

2. 接入技术的分类

目前的接入技术主要有几下几类:

(1) 铜线接入

铜线接入是指使用普通的电话铜线作为传输介质时的接入技术。为了提高原有铜线

的传输速率，必须采用各种先进的调制技术和编码技术。目前，电话通信网仍然是世界上应用最为广泛的网络，因此，许多人都致力于这方面的研究。铜线接入技术必须解决的是传输速率和传输距离之间的矛盾。常用的铜线接入技术如下：

① modem，电话线调制解调器接入，最大的数据传输速率为 56Kb/s。

② HDSL(high-bit-rate digital subscriber line)，高速数字用户环路接入，采用高速对称的 4 线 DSL。HDSL 可以在 2 对铜线上提供 1.544Mb/s(全双工方式)数据传输速率，具有安装简单、价格便宜的特点。

③ ADSL(asymmetric digital subscriber line)，非对称数字用户环路接入，采用频分复用技术，通过单对电话线路向用户同时提供语音电话和数据的服务。它可以为用户提供较高的数据传输速率，其下行方向的传输速率为 32Kb/s～8.192Mb/s，上行方向的传输速率为 32Kb/s～1.088Mb/s。

④ VDSL(very high-bit-rate digital subscriber line)，超高比特数字用户环路接入。它是一种极高速的数据传输技术，是在 ADSL 基础上发展起来的 xDSL 技术，其最大下行方向的传输速率为 55.2Mb/s，上行方向的传输速率为 19.2Mb/s。VDSL 有着较强的应用前景，它与 ADSL 一样，也采用了频分复用技术。发送时，它将普通电话 POTS、ISDN，以及 VDSL 的上下行信号放在不同的频带内发送出去；接收时，采用滤波器分离出各种信号。VDSL 目前仍处于研发之中，它实际上可视作 ADSL 的下一代技术，其平均传输速率可比 ADSL 高出 5 至 10 倍。另外，根据市场或用户的实际需求，VDSL 可以设置成对称的，也可以设置成不对称的。

(2) cable modem 接入

即有线电视同轴电缆调制解调器接入方式，其最大的下行方向传输速率为 30Mb/s，上行方向传输速率为 10Mb/s。目前，中国存在大约 8 000 万个有线电视用户，因此，这种接入技术被认为是信息高速公路中的优选方案之一。

(3) 光纤接入

光纤是目前传输带宽最宽的传输介质，被广泛地应用在局域网的主干网上。由于前面的两种接入技术各有优缺点，而光纤技术正在飞速地发展和普及，光纤网络的价格也在迅速下降，因此，光纤到户正在被人们接受和喜爱。

(4) 同轴电缆和光纤混合(HFC)接入

这是有线电视公司开发的一种基于 CATV 的光纤与同轴电缆的混合网络。HFC 是一种集电视、电话和数据服务于一体的宽带综合业务接入网。

用户的计算机、局域网与 Internet 的接入方式，从物理连接类型来考察，通常可以分为专线连接、局域网连接、无线连接以及电话拨号连接等几种。而按照应用规模通常将网络的接入技术分为普通用户和专线用户两种方式。下面将简单介绍各种常用接入方式的特点，实际工作中应根据自己的具体情况酌情选用。

2.4.2 普通用户、小型单位用户的接入技术

1. PSTN(电话拨号)用户的接入技术

普通用户和小型单位用户通常使用普通模拟电话线加 modem 接入到 ISP，即 PSTN

(电话拨号)接入方式。

(1) PSTN 的接入技术

计算机单机及使用代理服务器的 LAN 接入 Internet 的结构,参见图 2-1。该方式适用于数据通信量较小的单位局域网和个人微机使用。电话拨号上网的用户只需要具备一台调制解调器、一条电话线(外线或分机内线),普通的通信软件(单机接入)和代理服务器软件(LAN 接入),再申请一个 ISP 的上网账号即可使用。另外,电话拨号上网的用户还可以选择 PPP 或 SLIP 协议方式。常说的 PSTN 接入方式是指使用 modem 和 PSTN 线路拨号接入 Internet。

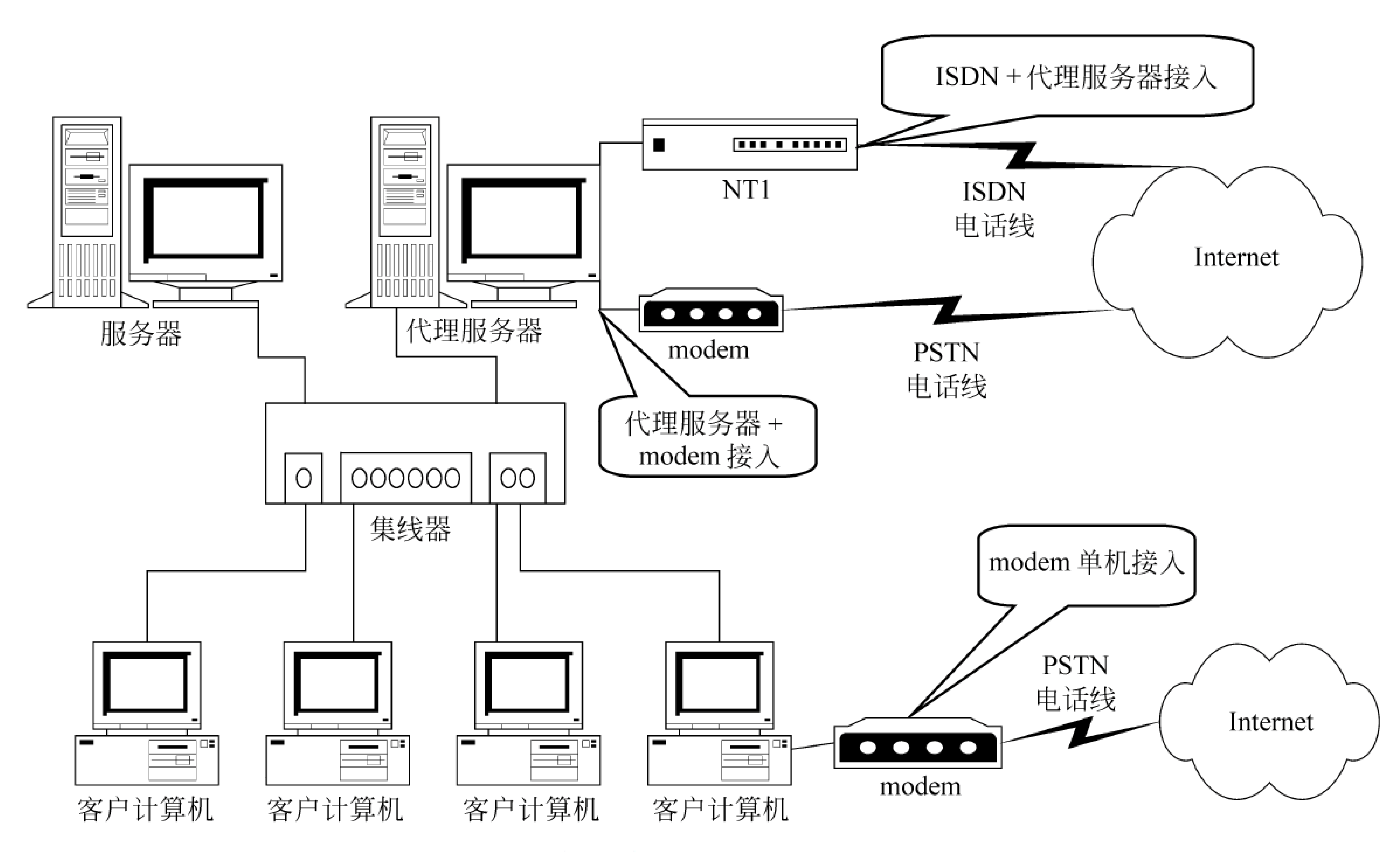


图 2-1 计算机单机、使用代理服务器的 LAN 接入 Internet 结构

(2) PSTN 用户支付的费用(拨号方式)

PSTN 用户的维持费用,分为上网电话费和上网费两个部分。

(3) PSTN 接入的应用特点

优点:所需设备简单,实现容易,投资和维持费用低廉。

缺点:速度低,传输信号质量低、性能差,可靠性不高。

2. ISDN 和 ADSL 电话专线用户的接入技术

通过公用通信网络的特殊接入设备和线路连入 ISP 或直接连入 Internet 的用户可以被统称为专线用户。在专线用户中,较流行的接入技术有以下几种:

(1) ISDN(又称窄带综合业务数字网)接入技术

ISDN 是在 IDN(综合数字电话网)基础上发展起来的一种先进的网络技术。ISDN 的主要目的是使用户至其他用户之间的数据传输全部数字化,它以数字化的方式处理各种业务。

ISDN 接入技术的最大优点是不需要架设专用网络,而利用当今世界上分布最广的

电话铜线作为传输介质。ISDN 所需设备较简单，费用较低，因此是普通用户、小型商务或小规模的单位推荐采用的接入方式。用户只要具备一台微机、一组 ISDN 终端接入设备(NT1 等)、一条 ISDN 电话线，就可以利用电话拨号上网。虽然采用的传输介质仍为双绞线，但最大的传输速率却可达 64Kb/s 或 128Kb/s。ISDN 接入不但可以实现多台计算机或终端共用一条 ISDN 电话线，还可以实现其他诸如语音、传真、图像等数据传输量较大的数据通信业务。

① ISDN 接入 Internet 的结构。

• 局域网用户“代理服务器”+“NT1”的接入结构。

硬件结构如图 2-1 所示，其中“NT1”为智能网络终端，可以为用户提供 2B+D(144Kb/s)的连接，ISDN 代理服务器由安装了代理服务器软件的计算机充当。该方案支持多个用户共用一条 ISDN 线路。它是目前小型单位经常采用的一种方案，也是投资、维护和运行费用最低的一种方案，因此，被认为是当前小型单位可采用的性能价格比较高的一种方案。

• 个人普通用户“NT1”接入结构。

硬件结构如图 2-2 所示，其中“NT1”为智能网络终端，为用户提供 2B+D(144Kb/s)的连接。该方案为普通“单机”或“双机”接入 Internet 时使用，不上网时，该方案可以提供两路语音线路。各种可能的组合方案有：两路 Internet、一路语音和一路 Internet、两路电话、一路电话一路传真等。

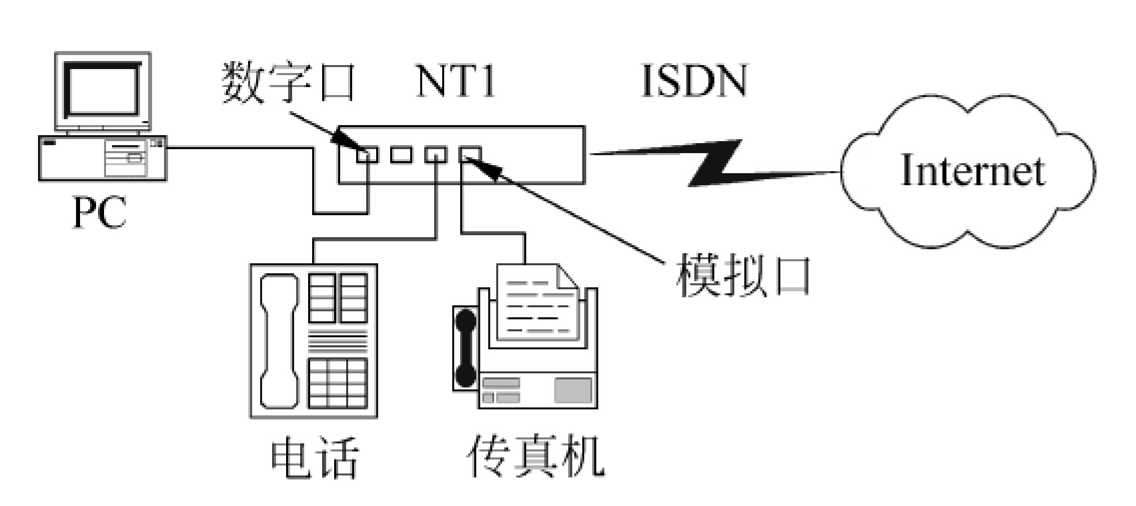


图 2-2 计算机单机使用 ISDN 接入 Internet 结构

• 局域网用户“路由器”+“NT1”的接入结构。

硬件结构如图 2-3 所示，其中局域网的交换机或集线器与路由器的 LAN 口相连。根据路由器支持 ISDN 线路的多少，可以为用户提供多倍“2B+D(144Kb/s)”的连接，例如，两条 ISDN 专线可以提供 2×144 Kb/s 的连接，可以实现 2×128 Kb/s 的数据传输带宽。

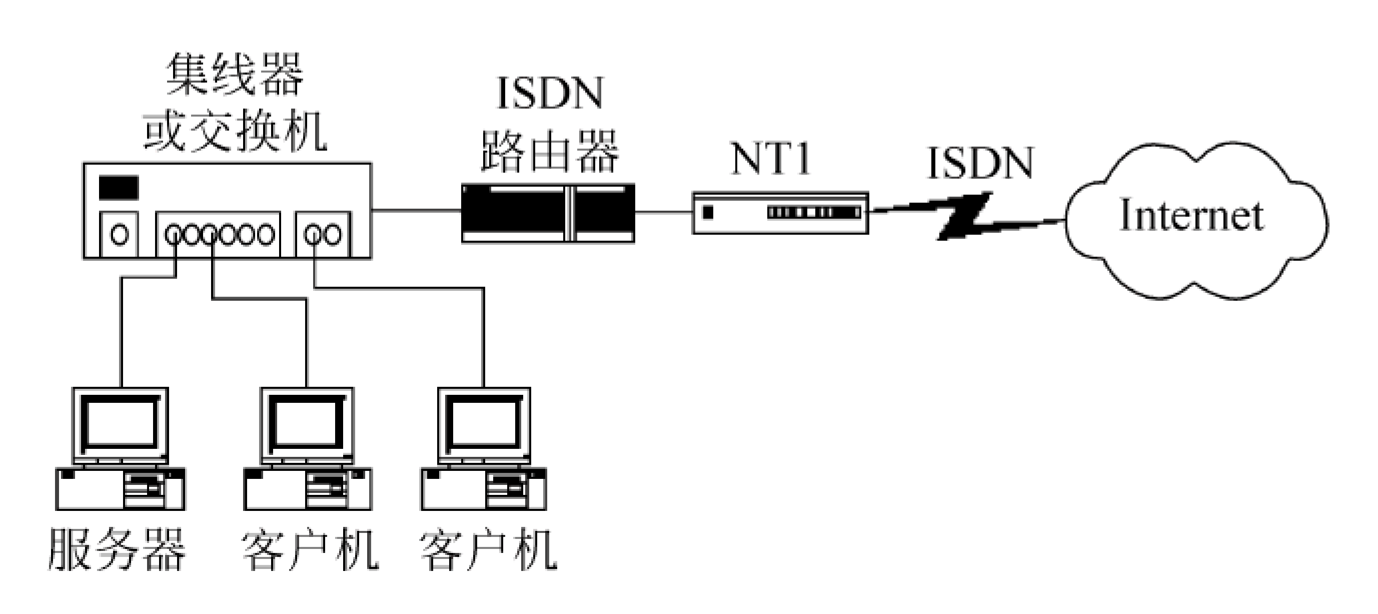


图 2-3 局域网使用 ISDN 路由器接入 Internet 结构

每个客户机通过 ISDN 路由器的代理与 Internet 连接。该方案不用设置代理服务

器，又支持多个用户共用一条 ISDN 线路，因此这是目前小型单位经常采用的一种方案，也是速度更高，投资、维护和运行费用较低的一种方案，被认为是当前小型单位可以选择采用的性能价格比较高的一种方案。

② ISDN 的应用特点。

- 全数字化线路、通话建立时间短、质量好、稳定性高。
- 线路使用效率高。一条 ISDN 线路可以实现一线带 3 机（PC、fax 和电话），三机共一线，但同时只可以使用其中的两条线。
- 接入速率比调制解调器高，适合语音、视频等多媒体数据的传输。
- ISDN 拨号上网可以节约大量日常通信费用。
- ISDN 的网上虚拟 DDN 比专线 DDN 更廉价和实用。
- 利用现有电话网络，使网络建设和改造费用降低。
- 兼容性好。可以保留原有 modem 上网的方式。

（2）ADSL 非对称用户专线接入技术

ADSL 使用普通电话线作为传输介质，虽然传统的 modem 也是使用电话线传输的，但传统的 modem 只使用了 0kHz～4kHz 的低频段，而电话线在理论上有接近 2MHz 的带宽。ADSL 正是使用了 26kHz 以上的高频带才能提供如此高的速度。

ADSL 接入技术的最大优点也是不需要架设专用网络，它充分利用了当今世界上分布最广的电话铜线作为传输介质，并利用多路复用技术，在一对铜质双绞线（电话线）上建立 3 个通信信道。ADSL 通过普通电话线传输数据的速度（8Mb/s）几乎比传统的调制解调器（56Kb/s）快 150 倍，比 ISDN（128Kb/s）快 60 倍。另外，使用 ADSL 接入技术时，线路有良好的抗干扰性能，在受到干扰的地方，它可以动态地调整通道的传输速率，而在未受干扰的地方或干扰小的地方，它可以保持较高的传输速率，同时它还可以把受干扰较大的子通道内的数据流转移到其他通道上，这样既保证了数据的高速传输，又保证了传输的质量。这一切主要归功于它的先进的调制解调技术。ADSL 设备的安装包括局端线路的调整和用户端设备的安装两个方面。

① 局端线路的调整。指将用户原有的电话线路接入 ADSL 的局端设备。

② 用户端设备的安装。当前，由于用户端 ADSL 设备是由电信部门提供并负责安装的，因此，对于广大用户来说，用户端的 ADSL 调制解调器的安装比普通的 modem、ISDN 终端设备的安装都要简单。其硬件和软件的安装过程如下：

- 将电话外线连接到滤波器上，滤波器的作用是分离语音和数字信号；
- 用一根 ADSL 电缆（两芯电话线）连接滤波器和 ADSL 调制解调器；
- 用一根两头接有 RJ-45 水晶头的 UTP 双绞线连接 ADSL 调制解调器和计算机上的网卡。此台计算机的另一个网卡接入局域网交换机成集线器；
- 设置好 TCP/IP 协议中的 IP 地址、DNS 卡和网关等参数。

使用 ADSL 接入 Internet 的结构如图 2-4（单机接入）和图 2-5（局域网接入）所示。

综上所述，许多专家都确信以 ADSL 为主的 xDSL 技术终将成为铜质双绞线上的主流技术，而目前常采用的普通 modem 的拨号接入，以及 ISDN 的接入技术都将逐步过渡到 ADSL 接入方式，最终的目标是实现光纤到户。

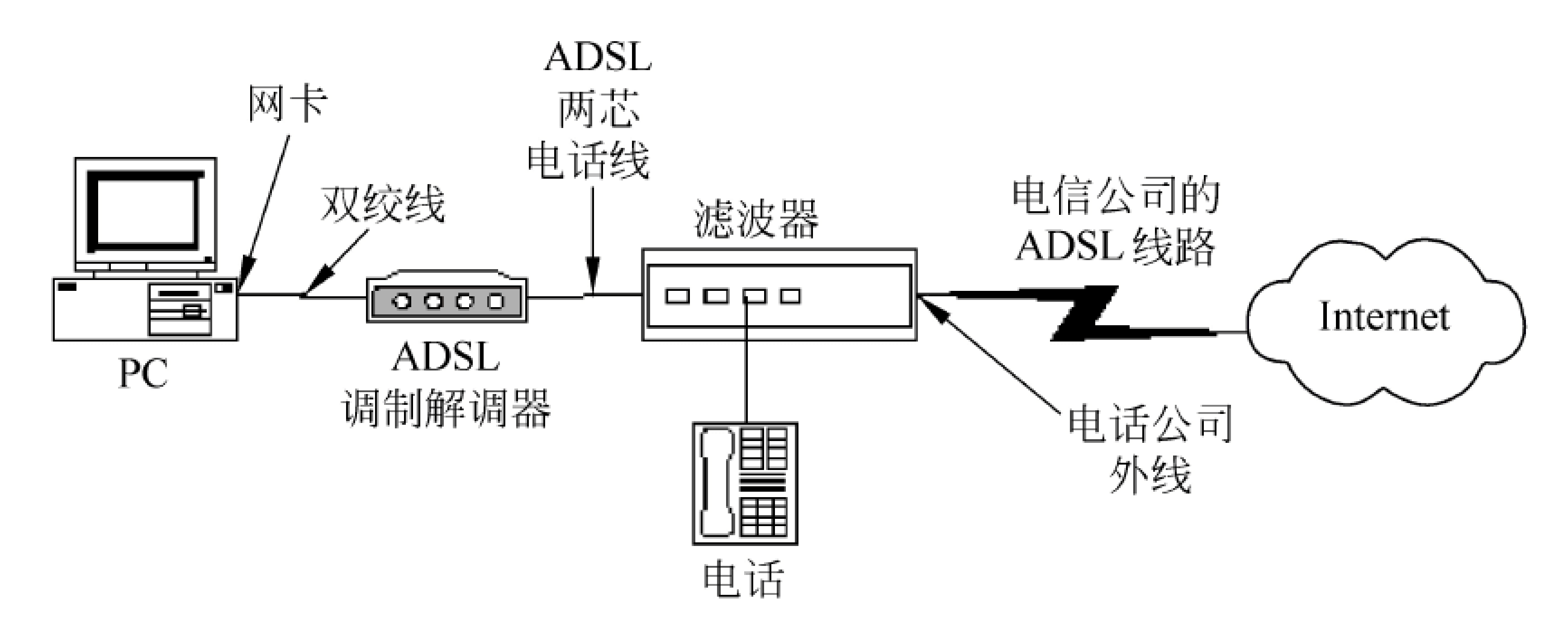


图 2-4　PC 机使用 ADSL 接入 Internet 的结构

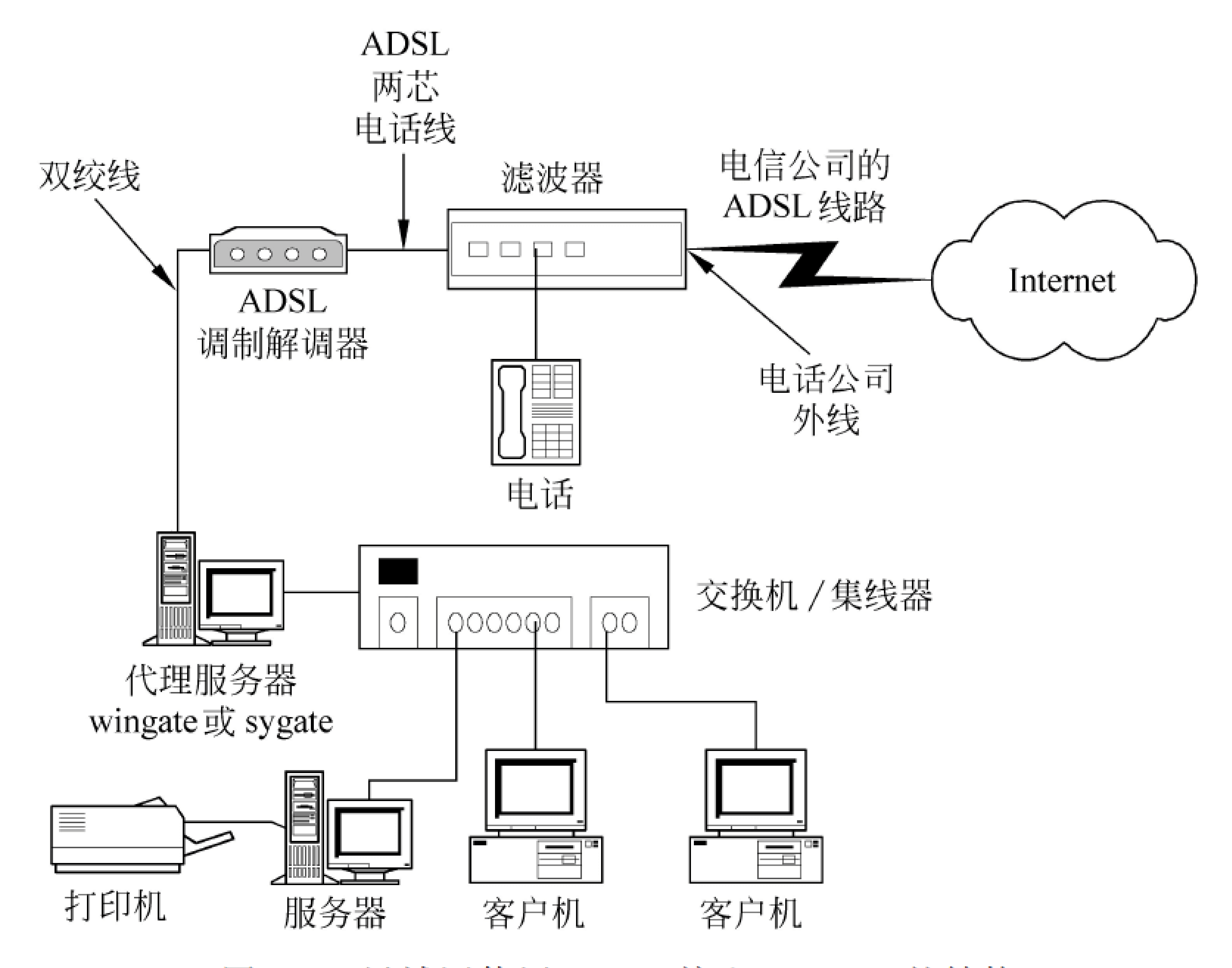


图 2-5　局域网使用 ADSL 接入 Internet 的结构

2.4.3　大公司及企事业单位用户的接入技术

较大的公司及企事业单位一般采用专线连接或局域网连接方式。这里主要指用户利用网络电缆将自己的计算机接入一个大型机构或单位已建立好的网络，这个网络再通过路由器或其他设备接入 Internet。

大公司及企事业单位用户的接入技术主要有拨号上网和通过公用数据网的数据专线上网两种方式，实例如图 2-6 和图 2-7 所示。

通过公用通信网的数据专线接入 Internet 时，可以租用或铺设专线，此线路由大型机构或单位独占，因此，称之为“专线”。

专线上网的优点是：通信速率高，适合于业务量大的网络用户使用，此外，接入 Internet 后，网上的所有用户均可以使用 Internet 提供的服务。

专线上网的缺点是：专线上网的用户需要专门的线路（专线）和路由器等专用设备，因此，一次投资、日常运行和维护费用都比较高。目前，常见的专线接入主要有以下几种类型：

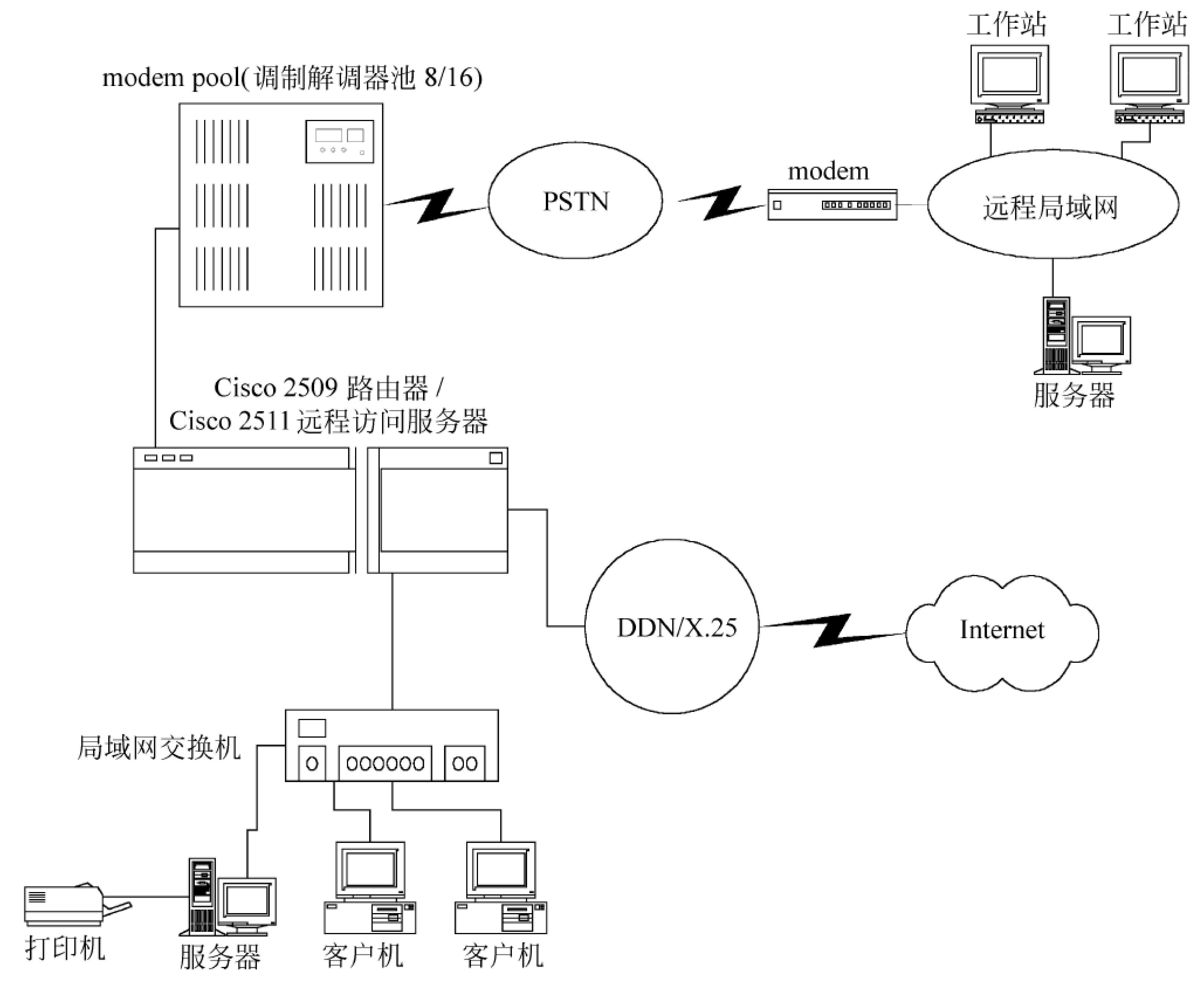


图 2-6　局域网的远程访问和使用拨号方式接入 Internet 的结构

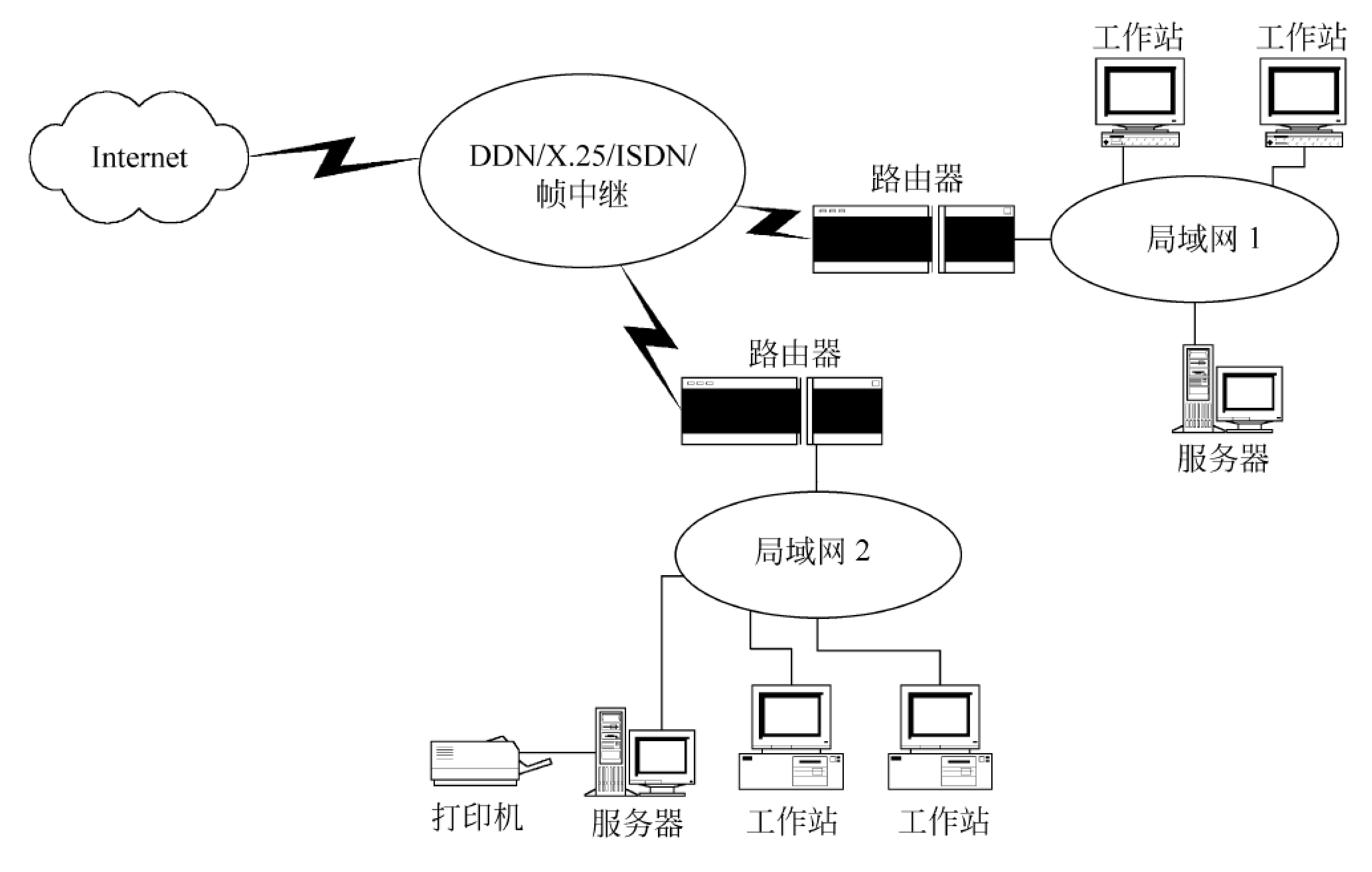


图 2-7　局域网使用数据网提供的数据专线接入 Internet 的结构

1. 帧中继接入技术

帧中继接入技术以简化网络规程、提高网络传输速度、缩小延时时间、提高吞吐量为目标，提供速率高达 1.54Mb/s～45Mb/s 的高速宽带业务服务。

2. DDN 接入技术

如前所述，DDN 是由光纤、数字微波或卫星数字传输通道和数字交叉连接的复用设备等专用设备组成的数字基干传输网络。它没有交换的功能，只有交叉连接的功能。DDN 向用户提供专用的数字数据的传输信道，支持点到点、点到多点的通信方式，并提供半永久的业务传输网，从而为用户建立专用数据网提供了条件，因此也称为专线数据网。电信部门利用 DDN 提供的电路构成了各种数据网和业务网，例如分组交换网等。

DDN 使用了多种传输介质，例如光纤、数字微波和卫星通信等，用户端可以使用普通的双绞线和同轴电缆。

（1）DDN 接入服务

DDN 的接入方式分为用户终端设备接入和用户网络接入两种方式。

① 用户终端设备接入方式。用户终端设备可以是计算机、图像设备，也可以是电话机和传真机。根据它们的接口速率和传输距离的不同，可以使用的接入方式如下：

- 模拟线路（模拟专用网加电话网）加调制解调器接入方式。当客户距离 DDN 较远时，可以采用这种在模拟专用网和电话网上开放数据业务的接入方式。其调制解调器可以采用基带或频带调制解调器，连接方式如图 2-8 所示。

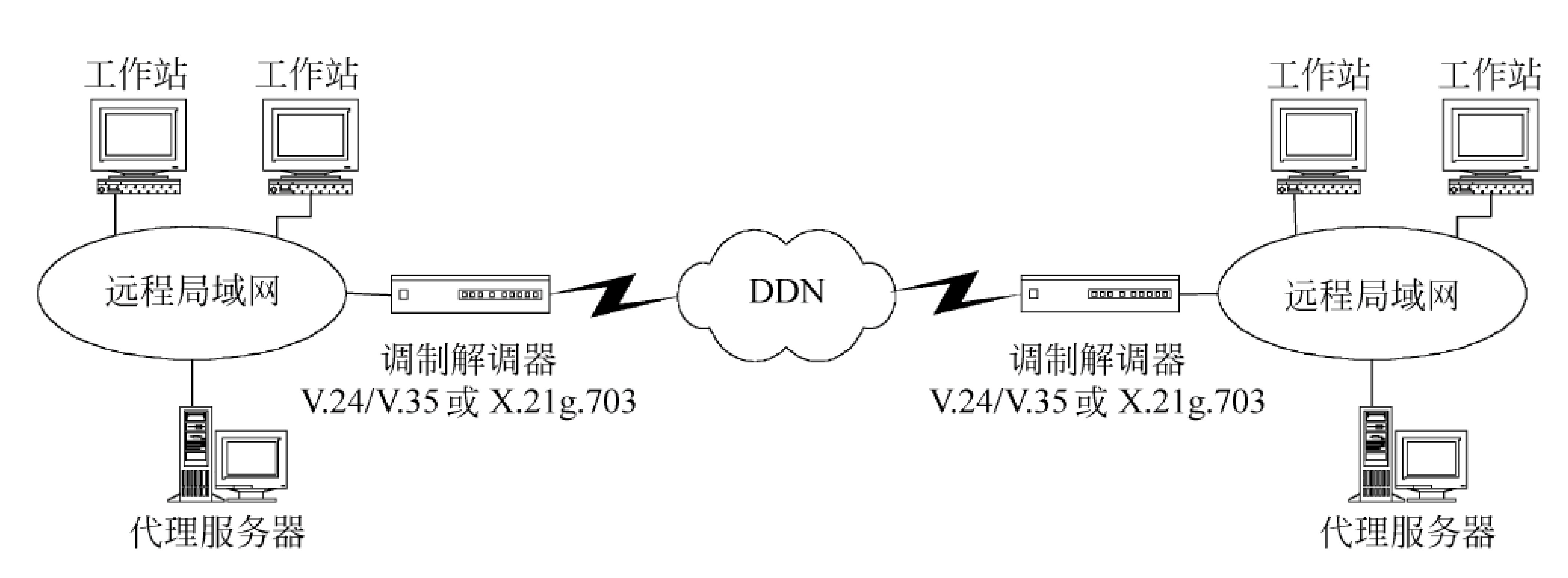


图 2-8　远程局域网通过 DDN 加调制解调器连接

- 数据终端设备接入方式。如图 2-9 所示，此时可以不必使用调制解调器，通过网管中心对其管理的远程数据终端设备进行远程配置、参数修改、日常维护和故障诊断，从而提高了系统的可靠性。
- 通过用户集中设备的接入方式。如图 2-10 所示，使用 DDN 小型复用器接入 DDN 网，实现各远程 LAN 的连接。这种方式采用 DDN 小型复用器进行远程计算机网络之间的连接，或者接入 Internet。该方式使用起来很灵活，不仅可以支持 2.4Kb/s、4.8Kb/s、9.6Kb/s 或者更高的数据传输速率，还可以支持话音和传真等业务。通过用户集中设备接入 DDN 网的方式，还可利用基群复用器等设备。

② 用户网络接入方式。如图 2-11 所示，这种接入方式主要指用户端局域网通过路由器接入 DDN 网，实现各远程 LAN 的连接，或者接入 Internet。在上述的局域网互联

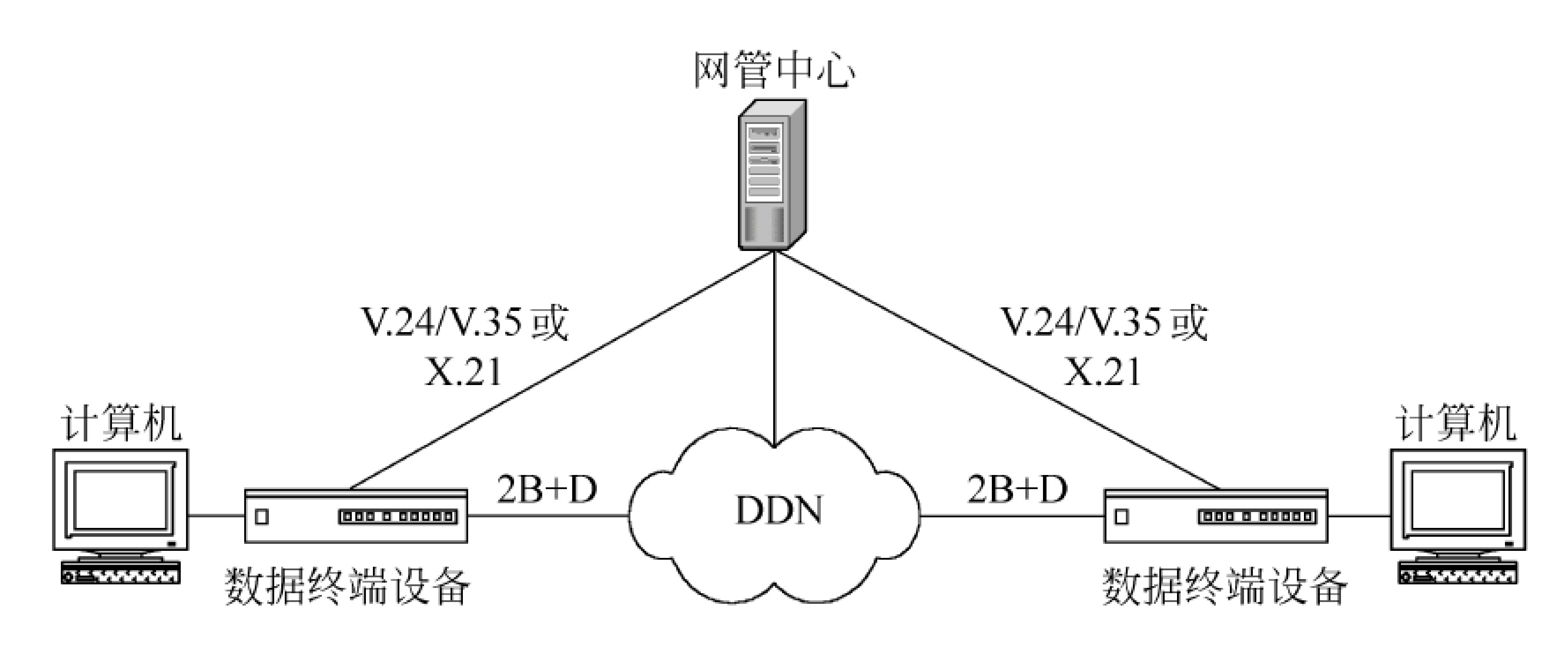


图 2-9　通过 DDN 加数据终端设备的连接

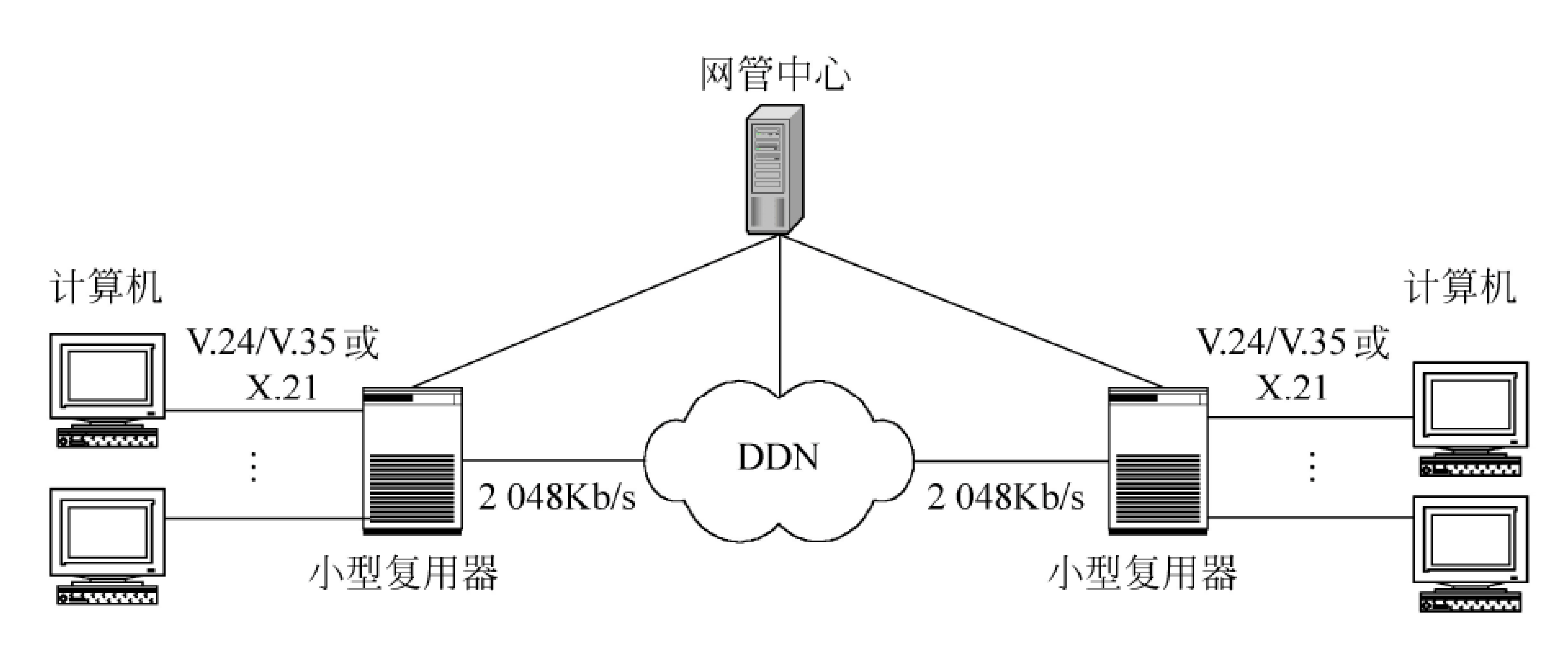


图 2-10　通过 DDN 加用户集中设备的连接

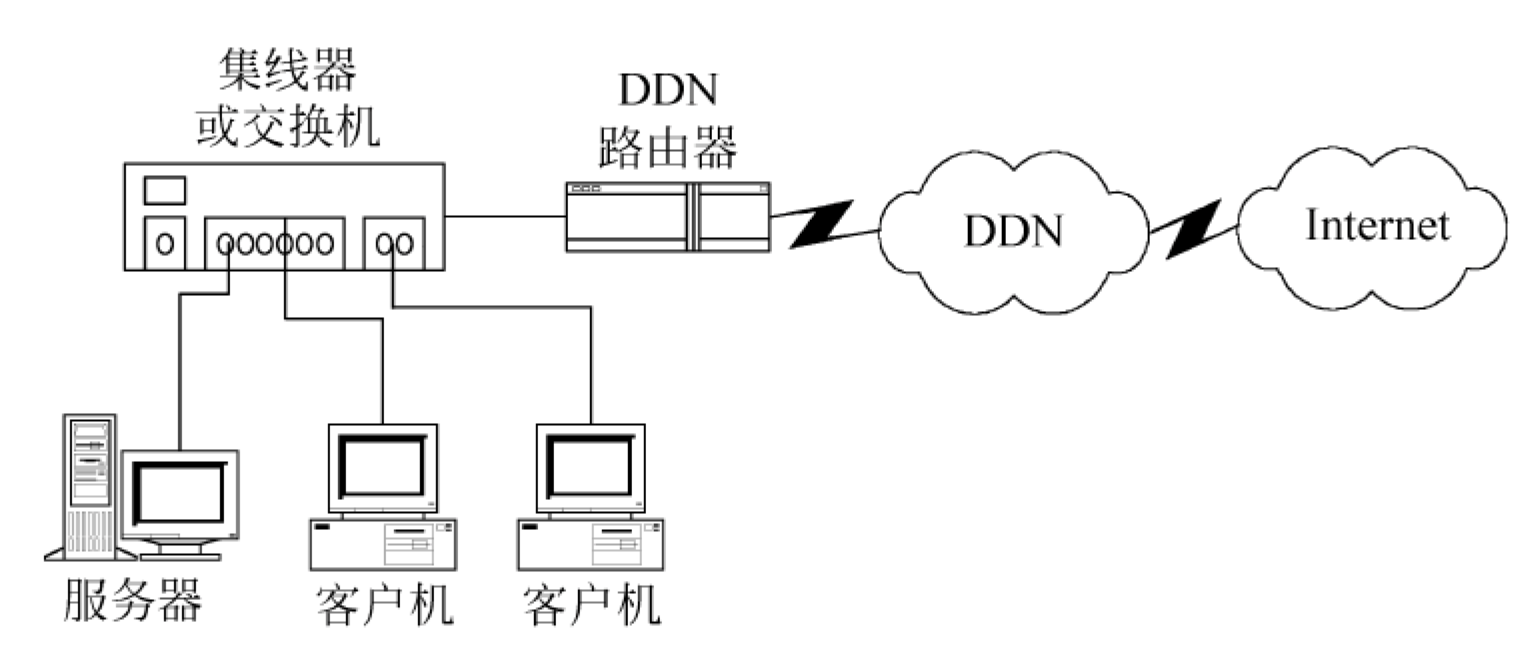


图 2-11　局域网通过 DDN 加路由器的连接

中，DDN 作为数据通信的支撑网络，可以为用户提供高速、优质的数据传输通道。此时，用户终端网络的接入方法有以下几种：

- 距离较近时，可以直接接入 DDN 网；
- 距离较远时，可以通过用户集中设备接入 DDN 网；
- 通过 2 048Kb/s 数字电路接入 DDN；
- 通过模拟电路接入 DDN。

DDN 提供的网络间互联的方法有如下几种：

- 局域网之间通过 DDN 互联；
- 分组交换网与 DDN 互联；
- 用户的交换网与 DDN 互联；

• 专用 DDN 与公用 DDN 互联。

(2) 专线用户接入 DDN 网的费用

目前,我国的 DDN 专线方式的通信速率通常为 64Kb/s,也可以根据需要租用合适速率的专线,最高为 2Mb/s。DDN 主要适用于业务量大、使用频繁、要求的传输质量高和速度快的,具有大量数据传输业务的大型企事业单位用户,例如银行、证券公司等。

DDN 专线的基本月租费,从 2 000～20 000 元人民币不等,因此,个人和中小企业一般很少采用。我国的"数字数据网"简称为 CHINADDN,即中国数字数据网。

3. 光纤接入技术

所谓光纤接入,主要指使用光纤为传输介质,采用的具体接入技术可以是不同的。常用的光纤接入技术可以分为光纤环路技术、光纤和同轴电缆的混合技术(HFC)两种。其中,光纤环路技术采用全光纤、全数字化的传输方式;HFC 技术的主干部分采用光纤,用户部分采用同轴电缆经各分支器接入终结点用户,因此降低了网络成本。例如,CATV(有线电视)网采用的就是 HFC 技术。

光纤接入可用于高质量、高宽带的应用环境,比如 DDN 专线(数字数据网)、B-ISDN(宽带综合业务数字网)与 ATM(异步传输模式)服务专线等,可以满足大客户的接入要求。由于光纤技术具有的各种特点,使得以光纤为介质的数据传输网络不断发展,并逐步成为现代通信技术的主流。

4. 用户接入技术的性能比较

综上所述,用户入网方式通常分为两类,即局域网接入方式和计算机接入方式,前者使用网桥或路由器接入网络,后者使用接入设备(modem 或 FRAD 等)接入网络。

使用最多的方式还是拨号上网,例如,利用 PSTN、ISDN 与 DDN 专线及相应设备拨号上网,各种性能和费用比较参见表 2-1。

表 2-1　PSTN、ISDN 与 DDN 专线上网比较表

比较项目	PSTN	ISDN	ADSL	DDN 专线
连接方式	拨号	拨号	拨号	专线
速率(b/s)	低于 56K	64K 或 128K	1M～8M	9.6K～2M
承载信号	模拟信号	数字信号	模拟信号	数字信号
传输质量	低	很高	很高	高
支持多任务	弱	强	强	弱
支持多媒体	弱	强	强	弱
一次性投入	低	较低	较高	高
使用费用	低	较高	较高	高
使用灵活性	按需连接	按需连接	按需连接	永久连接

习题

1. 问答题

(1) 什么是广域网? 它具有哪些主要特点?

(2) 广域网的类型有哪些?

(3) 广域网提供的通信服务有哪些?

(4) 什么是网络互联? 它是如何定义的?

(5) 网络互联的类型有哪些?

(6) 网络互联中常用的硬件设备有哪些? 各有什么特点?

(7) LAN 接入 Internet 时的首选设备有哪几种? 分别画出使用 PSTN、ISDN 和 DDN 时的用户端网络系统结构图。

(8) 如果用户安装了多个调制解调器,应当如何进行测试?

(9) 如果所安装的调制解调器发生了使用的资源冲突,即 I/O 或 IRQ 冲突,应当如何解决? 解决的步骤如何?

(10) 调制解调器除了拨号上网之外,还有什么功能?

(11) ISDN 的终端设备有哪几种?

(12) 计算机可以使用的 ISDN 设备有几种?

(13) 如何通过 ISDN 实现局域网与 Internet 连接?

(14) ADSL 的工作原理是什么? 使用 ADSL 上网的特点有哪些? 优势是什么?

(15) 在局域网中如何使用 ADSL 实现与 Internet 的连接? 又如何实现远程网络工作站与局域网的连接?

(16) DDN 的最高传输速率是多少? 对应的投入和运行费用分别为多少?

(17) DDN 接入的申请过程有哪些? DDN 的用户接入方式有哪几种? 所用的设备都是什么?

(18) 请经过调查写出局域网使用 DDN 接入 Internet 的过程。

2. 设计题

(1) 当一个中小型单位的 100Base-T 交换式局域网与 Internet 两个网连接时,使用何种接入技术? 请为其进行设计,并画出连接示意图。说明所设计方案的特色和主要性能指标,以及投资和维持费用的组成。

(2) 请为上述局域网中的远程工作站访问该局域网的方法进行选择和设计。画出的连接示意图,并说明主要互联部件的作用,维持费用的组成。

实训题目

1. 调制解调器实验

① 调制解调器的安装。

② 在 Windows 98/Me 中安装和设置调制解调器,并通过它拨号上网。

③ 处理调制解调器拨号上网的常见故障。

2. ISDN 实验

① ISDN 适配器的安装。

② 在 Windows 98/Me 中安装和设置 ISDN 适配器，并通过它拨号上网。

3. 代理服务器实验

① 安装和配置代理服务器，例如使用 WinGate。

② 配置代理服务器的客户工作站，例如 Windows 98/2000/XP 中 TCP/IP 协议的网关地址。实现 Internet 浏览和收发电子邮件。



第3章 Internet、Intranet 与 Extranet

在建设好局域网的物理网络之后，管理员应当清楚局域网、Internet 和 Intranet 之间的联系与区别，并掌握建设、规划和实现 Intranet 的过程和技术。

主要内容：

- Internet 中的基本概念、知识和术语；
- Internet 技术特点、主要应用和常用的术语；
- Internet 中的 WWW 技术；
- Internet、Intranet 和局域网的关系；
- Intranet（企业内联网）的定义、网络结构和技术特点；
- Extranet（企业外联网）的定义、网络结构和技术特点。

3.1 Internet 中的基本概念、知识和术语

3.1.1 Internet 的技术特点

1. Internet 的定义

Internet 的中文译名为因特网，也称为国际互联网。Internet 是使用公共语言进行通信的全球计算机网络。它类似于国际电话系统，本身以大型网络的工作方式相连接，但整个系统却又不为任何人所拥有或控制。

Internet 的简单定义：Internet 就是由多个不同结构的网络，通过统一的协议和网络设备，即通过 TCP/IP 协议和路由器等互相连接而成的、跨越国界的、世界范围的大型计算机互联网络。

2. Internet 的技术特点

Internet 通过 TCP/IP 协议将五花八门的计算机和网络连接起来。TCP/IP 是目前惟一可以供网络上各种计算机连接的通信协议集。Internet 技术主要包含以下几个方面：

① Internet 提供了当今时代广为流行的、建立在 TCP/IP 协议基础之上的 WWW（World Wide Web）浏览服务。

② 在 Internet 上采用了 HTML、SMTP 以及 FTP 等各种公开标准。其中,HTML 是 Web 的通用语言;SMTP 是电子邮件使用的协议;FTP 是文件传输协议。

③ Internet 采用的 DNS 域名服务器系统,巧妙地解决了计算机和用户之间的"地址"翻译问题。

3.1.2 Internet 的主要应用

Internet 是当今世界上最大的数据库和最经济的联络和沟通的手段。Internet 提供的常用服务类型如下:

1. E-mail(电子邮件)服务

电子邮件能够以非常高的速度被发送到世界上任何提供此服务的地方。理论上讲,可以即发即到,也就是说用户的电子邮件可以在瞬间发送到对方的邮件服务器上,在几分钟之内传递到收件人手中,而所需要的费用却是极其低廉的。

2. WWW 访问服务

通过使用 HTTP(超文本传输协议),人们使用各自的浏览器(如 IE、Netscape)便可以轻松地访问和浏览五彩缤纷的因特网世界。人们可以在最短的时间内了解到最新新闻、最新技术、最新时尚、最新产品等一切最新鲜的事物。

3. FTP(文件传输)服务

Internet 是一座装满了各式各样计算机文件的宝库,其中有许多免费和共享软件、二进制的图片文件,声音、图像和动画文件,当然还有各种书籍和参考资料。对于上述内容,可以采用几种办法传输到计算机上,其中最主要的办法就是通过 FTP(文件传输协议)。使用这项服务,人们坐在家中,就可以查阅和下载美国国家图书馆里的资料。通过 Internet 的 FTP 服务,大量的文件和共享软件可以迅速被传递,而在此过程中所使用的动态查询技术是传统手段无法比拟和实现的。

Internet 提供的其他服务还有:网络传真、IP 电话、电视会议、网上聊天和网络游戏等。总之,Internet 中与人们生活密切相关的信息服务、通信和娱乐等正在促进 IT 相关产业的高速发展,同时也正在影响着产业结构及相应人员结构的变化。

3.1.3 Internet 中常用的术语与 WWW 技术

1. **超文本标记语言(**hypertext markup language,HTML**)与动态网页**

① WWW 中的文档是通过超文本标记语言来描述的。WWW 文档被称为 HTML 文档,通常以".html"或".htm"为文件扩展名。HTML 是一种专门的编程语言,用于编制要通过 WWW 显示的超文本文件的页面。HTML 对文件显示的具体格式进行了详细的规定和描述。当浏览器读取 HTML 文件时,就会按照给出的命令去组成一个完整的页面。

② 动态网页是指使用 ASP、PHP 或 JSP 等网络程序设计语言设计和编写的网页,有时也称为动态 HTML 文件。用户在浏览网页时,可根据自身的需求在网页中进行输入、修改信息等交互式的操作,而网页会根据所输入的交互信息自动进行相应的变化,并产生更新后的网页。因此,凡是能够满足上述要求的、具有交互功能的网页,均可称为动态网页。

2. 超文本传输协议(hypertext transfer protocol,HTTP)

超文本传输协议是一种简单的通信协议,也是 WWW 上用于发布和浏览信息的主要协议。用户通过该协议,可以在网络上查询文件,而上述文件中又包含了用户可以实现进一步查询的多个链接。因此,用户可以只关心要检索的信息,而无需考虑这些信息的存储地址。为了从服务器上把用户需要的信息发送回来,HTTP 定义了其简单事务处理的 4 个过程。

- 客户与服务器建立连接;
- 客户向服务器递交请求,在请求中指明所要求的特定文件;
- 若请求被接纳,则服务器发回一个应答;
- 客户与服务器结束连接。

3. 环球信息网(World Wide Web,WWW)

WWW 简称 Web,也被称作“万维网”。Web 由许多 Web 站点构成,每个站点由许多 Web 页面构成,起始页叫做“主页”(home page)。WWW 通过超文本链接功能将文本、图像、声音和其他 Internet 上的资源紧密地结合起来,并显示在浏览器上。在超文本链接中,用户用鼠标单击链接处,就可以链接到另一处地理位置、页面完全不同的 Internet 资源中。链接的目标可以是同一服务器的当前 WWW 页面,也可以是 Internet 上的任何一处页面。

4. 主页(home page)、网页(web page)和超级链接(hyperlink)

(1) 网页的构成

WWW 上的页面通常被称为“网页”,也称为 Web 页面。如果把 Web 看作是图书馆,则 Web 站点就是一本书,而每一个 Web 页面就是书中的一页,主页就是书的封面。当人们访问某一个站点时,看到的第一个页面被称为该站点的“主页”(首页),而其他的网络页面则被称为“网页”。这些页面可以包含 4 种基本元素,即文本(text)、图像(image)、表格(table),以及超级链接(hyperlink)。

(2) 超级链接、超文本(hypertext)和超媒体(hypermedia)

① 超级链接:又称“超链接”。超链接就是已经嵌入了 Web 地址的文字、表格或图形。它是 HTML 语言中的重要元素之一,用来连接各种 HTML 元素和其他网页。

② 超文本:就是指具有了超级链接功能的文件。通过超文本上的超级链接点,可以跳转至其他位置。这些位置可包括硬盘上的其他文件(如 Microsoft Word 文档或 Microsoft Excel 工作表)、因特网或局域网、Internet 地址(如 http://www.microsoft.com)、书签或幻灯片。“超链接”的作用域为所提示的文字,一般为蓝色并带下划线,用户单击“超链接”处,就可以跳转至其指定的位置。编辑超文本时,单击“插入”菜单中的“超级链接”命令,即可插入超级链接。

③ 超媒体:就是包含有文字(text)、影像(movie)、图片(image)、动画(animation)、声音(audio)等多种信息的文件。

(3) 浏览器(browser)与网页浏览

浏览器是指安装在计算机上,用来显示指定文件的程序,常用的浏览器有微软的 Internet Explorer(即 IE)和 Netscape 公司的 Navigator。

WWW 的工作原理就是通过网络客户端的浏览器，去浏览指定的文件。世界各地的人们，可以将他们的 Web 网页置于世界任何地方的计算机上。Web 上的文件或页面通过超级链接而互相联系。在浏览器上通过单击特定的文本或图形，即带有超级链接的网页（超文本文件）就可以链接到其他页面。因此，当通过浏览器链接 Web 页面时，正是通过这些带有链接的网页来访问全世界范围内的各种信息。

5. 统一资源定位器（uniform resource locator，URL）

（1）URL 用来表示 Internet 或 Web 的地址

每个 Web 页面，包括 Web 节点的网页，均具有惟一的存放地址，这就是统一资源定位器 。这是一种用于表示 Internet 上信息资源地址的统一格式。通俗地说，URL 可以用来指定某个信息所在的位置和使用方式。URL 不但指定了存储页面的计算机名、确切路径，而且还给出了此页面的存取方式。

（2）标准的 URL 的组成

① 协议名。协议是使计算机之间能交换信息的一组规则和标准。

② 站点的位置。

③ 负责维护该站点的组织的名称。

④ 标识组织类型的后缀。例如，“.com”表示商业组织等。

⑤ 有时，URL 除了上述信息之外还提供服务器接入时的通讯端口号码。

（3）URL 的标准语法形式

URL 的标准语法形式可以用下列形式表示：

＜协议＞://＜信息资源地址＞[:网络端口 / ＜文件路径＞]

注：“[ ]”内的内容可以默认。如果默认，即使用系统的默认值。上述各项的解释如下所述。

① 协议　表示服务器所使用的通信协议。在 Internet 中，常用的通信协议及其定义如表 3-1 所示。

表 3-1　通信协议定义及服务性质

通信协议	协议名称及定义	默认端口编号	URL 的服务性质
HTTP	超文本传输协议	80	WWW 上的超文本服务
FTP	文件传输协议	21	因特网中交互式文件传输服务
File	本地计算机上的超文件传输协议		本地计算机的超文本服务
SMTP	访问 SMTP 邮件服务器的协议	25	因特网中电子邮件传送服务
RIP	路由信息协议		网络设备之间交换路由信息
DNS	域名服务协议	53	网络设备名字到 IP 地址的映射服务
News	网络新闻传输协议		Usenet 网络新闻组访问服务
Telnet	远程登录协议（网络终端协议）	23	因特网中远程登录服务

② 信息资源地址　是指存放文件的主机地址，也叫域名，此处也可以直接键入该主机的 IP 地址。它指明了这台主机所处的国家、网络和计算机的地址。

③ 网络端口　表示服务器使用的通讯端口编号，通常不同类型的服务使用不同的端

口编号。

④ 文件路径　根据查询的不同,在 URL 中,这一部分有时可以没有。如果需要指定文件路径,则应指出存放文件的地址和文件名。

例如,在 IE 浏览器的 URL 地址栏中键入“http://news.sohu.com/14/33/news147583314.shtml”,其中各信息的意义如下:

- “http://”　表示使用超文本传输协议查询信息;
- “news.sohu.com”　表示“sohu”网站主机的域名;
- “/14/33/news147583314.shtml”　表示该网站的新闻主页在主机上的路径和文件的具体名称。

6. IP 地址、域名(主机名)和 DNS(domain name system,域名系统)

① IP 地址　是 Internet 中使用的一种地址。访问 Internet 时,可以使用 IP 地址来访问 Internet 中的各种资源。IP 地址是由 4 段十进制数字组成的,它们代表了 32 位二进制数字,例如 168.160.226.2。

② 域名(domain name,DN,也称为主机识别符或主机名)　由于数字型的 IP 地址很难记忆,所以现在 Internet 中实际上使用的是直观明了的、由字符串组成的、有规律的、容易记忆的名字来代表因特网上的主机,这种名字称为域名,它是一种更为高级的地址形式。

③ DNS　DNS 担负着将形象的域名翻译为数字型 IP 地址的工作。

综上所述,IP 地址、域名(DN)和域名系统(DNS)担负着因特网上计算机主机的惟一定位工作。也就是说,在因特网上无论用户给出计算机主机的“IP 地址”或“域名”,DNS 都可以帮助用户找到这台主机。

3.2　Internet、Intranet 和局域网

Internet、Intranet 和局域网的关系,以及与其相关的基本概念是 Intranet 管理员应当深刻理解和掌握的基本知识。

3.2.1　Intranet(企业内联网)

对于一个企业来说,其 Intranet 的系统逻辑结构如图 3-1 所示。

1. Intranet 的定义

Intranet 通称为企业内联网,又称企业内部网,虽然它并非只用于企业,但却被简称为“企业网”。“Intranet”由于在其局域网内部采用了 Internet 技术而得名。因此,Intranet 可以定义为:由私人、公司或企业等利用 Internet 技术及其通讯标准和工具建立的内部 TCP/IP 信息网络。

2. Intranet 的技术特点

如图 3-1 所示,通常的 Intranet 都连入了 Internet;另外一些 Intranet 虽然没有连入 Internet,但是却使用了 Internet 的通讯标准、工具和技术。例如,某公司组建的内部网络

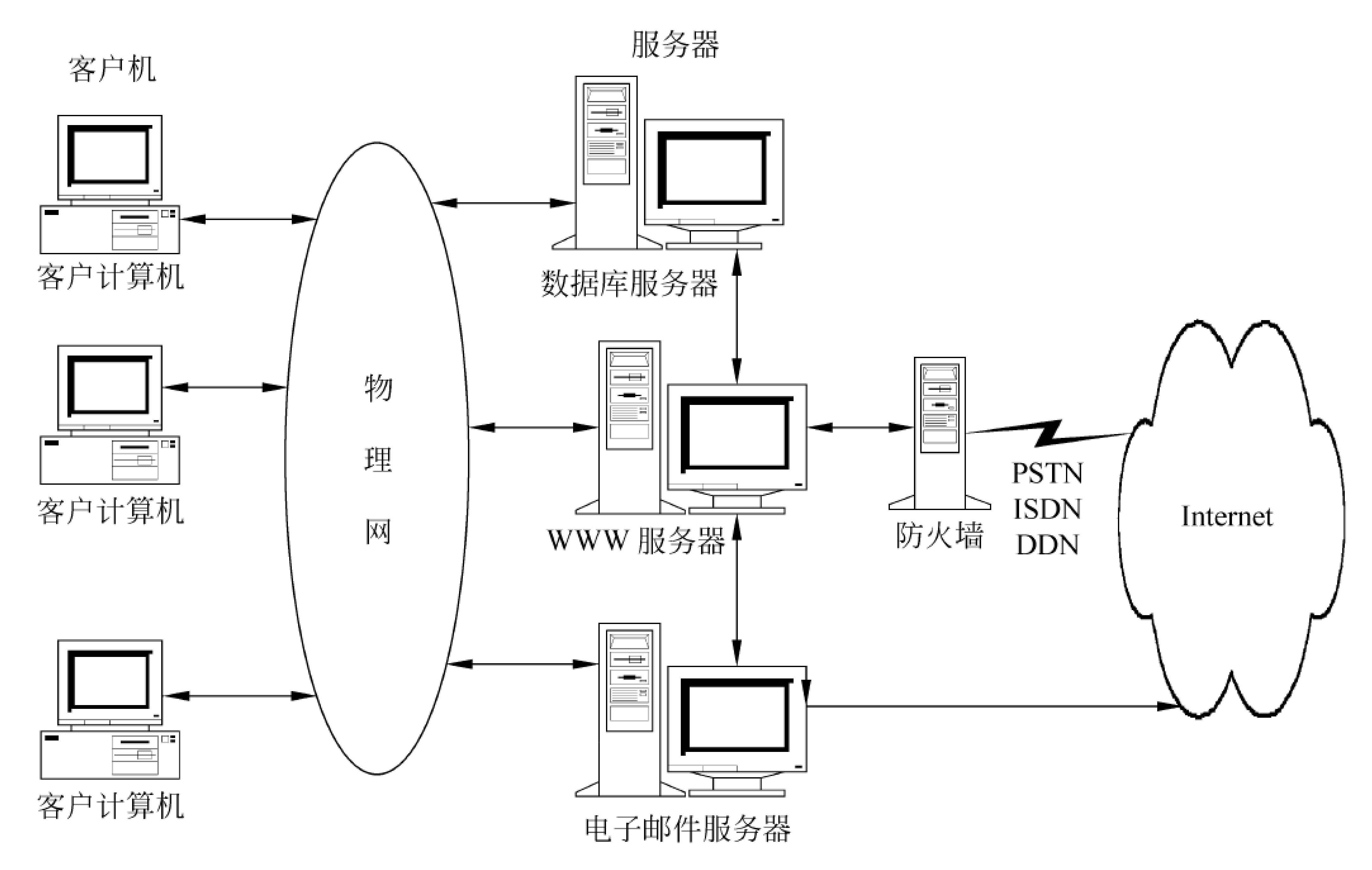


图 3-1　Intranet 的逻辑结构

与 Internet 一样都使用了 TCP/IP 协议，安装了 WWW（Web）服务器，用于内部员工发布公司业务通讯、销售图表及其他公共文档。公司员工使用 Web 浏览器可以访问其他员工发布的信息，因此，这样的网络也称为 Intranet。Intranet 的基本技术特点除了与 Internet 类似的 3 点之外，还有以下几个方面：

① Intranet 是把 Internet 技术应用于企业内部管理的网络。

② Intranet 提供了 6 项基于标准的服务：文件共享、目录查询服务、打印共享管理、用户管理、电子邮件和网络管理。

③ Intranet 具备了 Internet 的开放性和灵活性，它在服务于内部的同时，又可以对外开放部分信息。

3. Intranet 的网络结构

随着 Internet/Intranet 的广泛使用，计算机"网络化"和"信息化"是当今企事业单位发展的总趋势。由于企事业单位的经营、生产和运作方式的改变，网络技术迅速普及并飞速发展，随之而来的是 Web 技术的出现和发展。如今，C/S 网络结构已经发展为新的 B/S 形式。

（1）Intranet 采用的 B/S（浏览器/服务器）网络结构

B/S 的全称为 browser/server，是 C/S 结构发展的新模式。Intranet 采用的网络模式就是 B/S，它是一种 3 层的结构网。

B/S 结构的客户端采用了人们普遍使用的浏览器，因此，它是一个简单的、低廉的、以 Web 技术为基础的"瘦"型系统。其服务器端除了原有的服务器外，通常增添了高效的 Web 服务器。这就是 1996 年以后开始出现并迅速流行的 B/S 结构。B/S 的体系结构和网络结构如图 3-2 所示。



图 3-2 B/S 3 层模式的体系结构示意图

基于 B/S 模式的网络信息系统，通常采用 3 层或更多层的结构，即“客户机浏览器—Web 服务器—数据库服务器”。这种网络的中间件很多已被集成在 Web 服务器，其 B/S 模式以 Web 服务器为系统的中心，用户端通过其浏览器，向 Web 服务器提出查询请求（HTTP 协议方式），Web 服务器根据需要通过中间件向数据库服务器发出数据请求。数据库则根据查询或查询的条件返回相应的数据结果给 Web 服务器上的中间件，最后 Web 服务器将结果翻译成为 HTML 或各类脚本语言的格式，并传送给客户机上的浏览器，用户通过浏览器即可浏览自己所需的结果。

（2）使用“中间件（middle-ware）”的原因

尽管采用 C/S 模式有很多优点，但是对于大多数从事应用程序开发的人员和普通用户的程序开发人员来说，在 C/S 模式中必须编写跨越平台、多协议、多编译语言的网络应用软件，这是一件十分困难的事情。另外，如果程序开发人员需要针对底层网络协议编写程序的话，会使程序具有以下两个明显的问题：程序过多地依赖底层网络技术；程序很难集成新的网络服务。

基于 C/S 模式开发出的程序，将过多地依赖于网络协议和网络软件，而不利于程序的编写和维护，同时，也不利于程序的移植。为了解决应用程序对网络的过分依赖问题，C/S 模式在其发展的过程中，引入了“中间件（middle-ware）”的概念，同时将网络模式逐步发展为 B/S 模式。

（3）使用“中间件”的 B/S 模式的特点

B/S 模式的浏览器，访问数据库时为 3 层方式。它与 C/S 结构的 2 层结构相比，具有以下一些特点：

① 客户端软件成本低，易于更新和改动，用户可以自行安装浏览器软件，并使用通用的浏览器进行访问，与网络平台完全无关。

② 提高了网站系统的性能。中间件可以对服务的进程进行管理，使得一个服务进程能够处理多个用户的访问请求，而不像 C/S 结构中那样每个服务进程只能处理一个访问请求。当访问请求的数量超过服务器的处理极限时，中间件还会利用队列的缓冲机制，把服务器未能及时处理的请求放入队列中，等待服务器空闲时再进行处理。

③ 提高了数据库的响应速度。通过中间件，服务进程与数据库之间一直保持着连接，因此，当用户访问网站的信息系统时，大大减少了与数据库的连接次数和时间，从而有效地解决了由于数据库的频繁连接而导致的数据库性能下降的问题。

④ 提高了应用系统的安全性。中间件将客户端与数据库隔离起来，因此，客户端无权直接访问数据库，因而，十分有利于网站的安全管理，可有效地防止恶意的攻击。此外，还可以利用中间件的安全管理性能进行权限的控制与管理。

⑤ 提高了网站系统的扩充能力。采用中间件时，如果需要提高系统的性能和处理速度，可以随时扩充中间层的应用服务器的数量或能力，以分担部分应用服务。

4. Intranet 的特点

Intranet 具有以下一些显而易见的特点：

① Intranet 是一种企业内部的计算机信息网络。

② Intranet 是一种利用 Internet 技术开发的开放式计算机信息网络。

③ Intranet 采用了统一的基于 WWW 的服务器/浏览器(B/S)技术去开发客户端软件。因此,Intranet 中用户使用内部信息资源的方式和友好、统一的用户界面均与使用 Internet 时类似。文件格式具有一致性,有利于系统间的交换。

④ Intranet 使用的基于浏览器的瘦客户技术,成本低,网络伸缩性好,简化了用户培训的过程。

⑤ Intranet 改善了用户的通信和交流环境,例如,其用户可以方便地使用和访问 Internet 上提供的各种服务和资源,同时 Internet 上的用户也可以方便地访问 Intranet 内部开放的不保密资源。

⑥ Intranet 为企业管理现代化提供了途径。例如,在企业内部不但可以传送电子邮件、各种公文、报表和各种各样文档,还可以实时传递"在线"的控制和管理信息,召开多媒体网络会议,使得企业的无纸办公成为可能。

⑦ Intranet 一般具有安全防范措施。例如,企业内部的信息一般分为两类,一类是供企业内部使用的保密信息;另一类是向社会开放的公开信息,如产品广告和销售信息等。为了保证企业内部信息及网络的安全性通常需要使用防火墙等安全装置。

5. WWW 技术是 Intranet 的核心

Intranet 的核心技术是 WWW。WWW 是一种以图形用户界面和超文本链接方式来组织信息页面的先进技术,它的 3 个关键组成部分是 URL、HTTP 和 HTML。Intranet 的几个基本组成部分如下所述：

① 网络协议　TCP/IP 协议为核心。

② 硬件结构　以局域网的物理网络为网络硬件结构的基础。选择一定的接入技术与 Internet 互联。

③ 软件结构　其软件结构由浏览器、WWW 服务器、中间件和数据库组成。

由于构建、使用和管理 Intranet 是本书的一个重点,因此,关于规划、设计和实现 Intranet 的方法,以及有关 WWW 的技术等问题将在后续章节作详细介绍。

3.2.2　Internet 和 Intranet 的关系

1. Internet **和** Intranet **的联系**

① Intranet 是利用 Internet 技术组建的企业内部网络,Intranet 要与 Internet 互联才能更好地发挥作用,真正成为开放的计算机信息网络。Intranet 所使用的主要技术与 Internet 一致,它使用的 WWW、电子邮件、FTP 和 Telnet 等都与 Internet 一致,这是 Internet 和 Intranet 的主要共同之处。

② Intranet 采用统一的基于 WWW 浏览器的技术来开发用户端软件。因此,Intranet 用户使用的用户界面与 Internet 普通用户使用的界面、软件都是相同的。因而,Intranet 用户可以方便地访问 Internet 上提供的各种服务和资源;同时 Internet 用户也可

以方便地访问 Intranet 上的允许访问的各种资源。

总之，二者使用了相同的技术和应用方式，Intranet 只有通过与 Internet 互联才能更加充分地发挥自身的作用。

2. Internet 和 Intranet 的区别

① Intranet 是属于某个企事业单位部门自己组建的内部计算机信息网络，而 Internet 是一种面向全世界用户开放的不属于任何部门所有的公共信息网络，这是两者在功能上的主要区别之一。

② Internet 允许任何人从任何一个站点访问其中的资源，而 Intranet 上的内部保密信息则必须严格地进行保护。为此，Intranet 一般通过"防火墙"与外网（Internet）相连。

③ Intranet 内部的信息分为两类，一类是企业内部的保密信息；另一类是向社会公众开放的企业产品广告等信息。前一类信息不允许任何外部用户访问，而后一类信息则希望社会上广大用户尽可能多地访问。

3.2.3 局域网与 Intranet 的关系

1. 局域网（LAN）和 Intranet 的联系

（1）局域网和 Intranet 都是企业内部的私有网络

如前所述，局域网通常是指没有和 Internet 相连的，以普通方式工作的企业内部私有网络；而 Intranet 是一种可以根据自身需要选择与 Internet 相连还是断开，并且以 Internet 方式工作的企业内部私有网络。

（2）网络内部的组成与结构类似

两种网络的内部网络的物理结构类似，两种网络组建时都遵循局域网的设计规则和实施方法。

（3）网络内部的基本网络服务类似

两种网络中所能提供的 6 项标准服务基本相同，例如，均有文件共享、目录服务、打印共享管理、用户管理、电子邮件服务和网络管理几项服务。

2. 局域网逐步发展为 Intranet 的原因

目前，由于信息共享、信息交流和通信协作的需要，越来越多的局域网需要与外界相连而成为 Intranet。其主要原因如下：

① 企业内部需要与外界相互沟通，例如，企业内部信息的一部分，如产品广告和销售信息等，将允许外部计算机的随时访问。

② 企业内部的计算机也需要通过 Internet，及时了解外面的市场行情和各种信息，并通过因特网与外界进行廉价、快速的联系。

③ 企业内部的信息网络正在从 C/S 结构向 B/S 结构转向，即企业内部与外部将会以相同的浏览器工作方式进行信息的浏览和查询。

④ 多个 Intranet 需要联合经营，并以 Extranet（企业外联网）方式工作，实现有限资源的共享。

3. 局域网和 Intranet 的区别

（1）共享信息的性质不同

传统局域网中的信息均为企业内部的信息；而 Intranet 内的信息分为两类，一类是企业内部的保密信息；另一类是向社会公众开放的企业产品广告等公用信息。

(2) 安全性能的要求不同

LAN 中的资源共享一般局限在网络内部，而 Intranet 中的共享资源一般允许外部的有条件访问，因此，内部网络通常通过“防火墙”与外网(Internet)相连。所以，两种网络对安全性能的要求不同。

(3) 使用的技术要求不同

局域网可以仅使用局域网许可的标准构建，而并不要求一定使用 Internet 技术构建；而 Intranet 一般使用与 Internet 相同的技术构建。例如，Intranet 也会提供与 Internet 类似的多项基于标准的基本服务，如信息浏览(WWW)和电子邮件 E-mail 等。

(4) 具有的功能不同

LAN 通常只是一个局部的互联网络，一般只要能够互相通信并连接到一起，就可称为局域网。而 Intranet 对功能的要求则要强得多。

3.2.4 Extranet(企业外联网)

1. Extranet **的定义**

Extranet 一词来源于 extra 和 network，这两个单词组合之后定义的中文名称为“外部网”。由于 Extranet 的本质是对 Intranet 的延伸和扩展，因此，目前普遍使用“企业外联网”或“企业外部网”来定义 Extranet。

Extranet 是一个用 Intranet 和 Internet 技术构造的外部网络，它是一种使企业与客户、企业与企业互联而成的，为了完成共同目标的合作网络。

Extranet 将企业 Intranet 进一步扩展到合作伙伴，从而形成了企业之间相关信息共享、信息交流和相互通信的介于 Internet 与 Intranet 之间的网络。

2. Extranet 的网络结构

Extranet 与 Intranet 类似，涉及到主干网、网络互联设备、网络管理、网络服务器和客户机等设施。Extranet 分为开放型和专用型两种类型。

(1) 开放型 Extranet

典型的开放型 Extranet 网络结构如图 3-3 所示，这种类型的 Extranet 具有以下特点：

① 优点　各相关的企业都可以通过公用的 Internet 来构建企业的 Extranet，因此，具有成本低，组网灵活和开放性好等优点。凡是连接到 Internet 的用户均可以与之相连。

② 缺点　Extranet 中各企业 Intranet 的网络安全是它的棘手问题。

(2) 专用型 Extranet

专用型 Extranet 使用专用的数据通信信道来连接重要的合作伙伴，其典型的网络结构如图 3-4 所示。

3. Extranet 网络的构建

Extranet 网络构建时，通常使用下述两种方法。

(1) VPN(虚拟专用网)方式

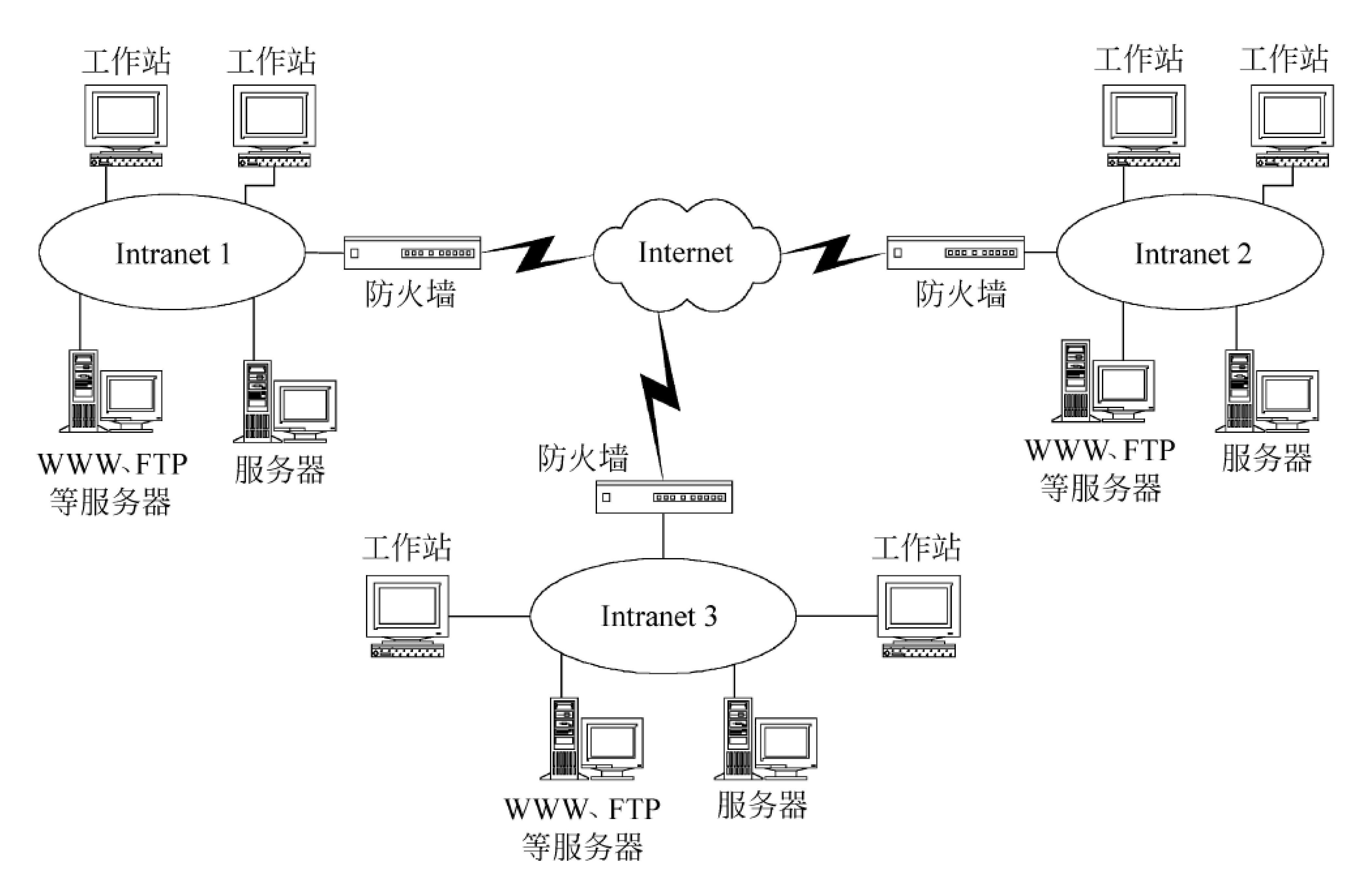


图 3-3　开放型 Extranet 的网络系统结构

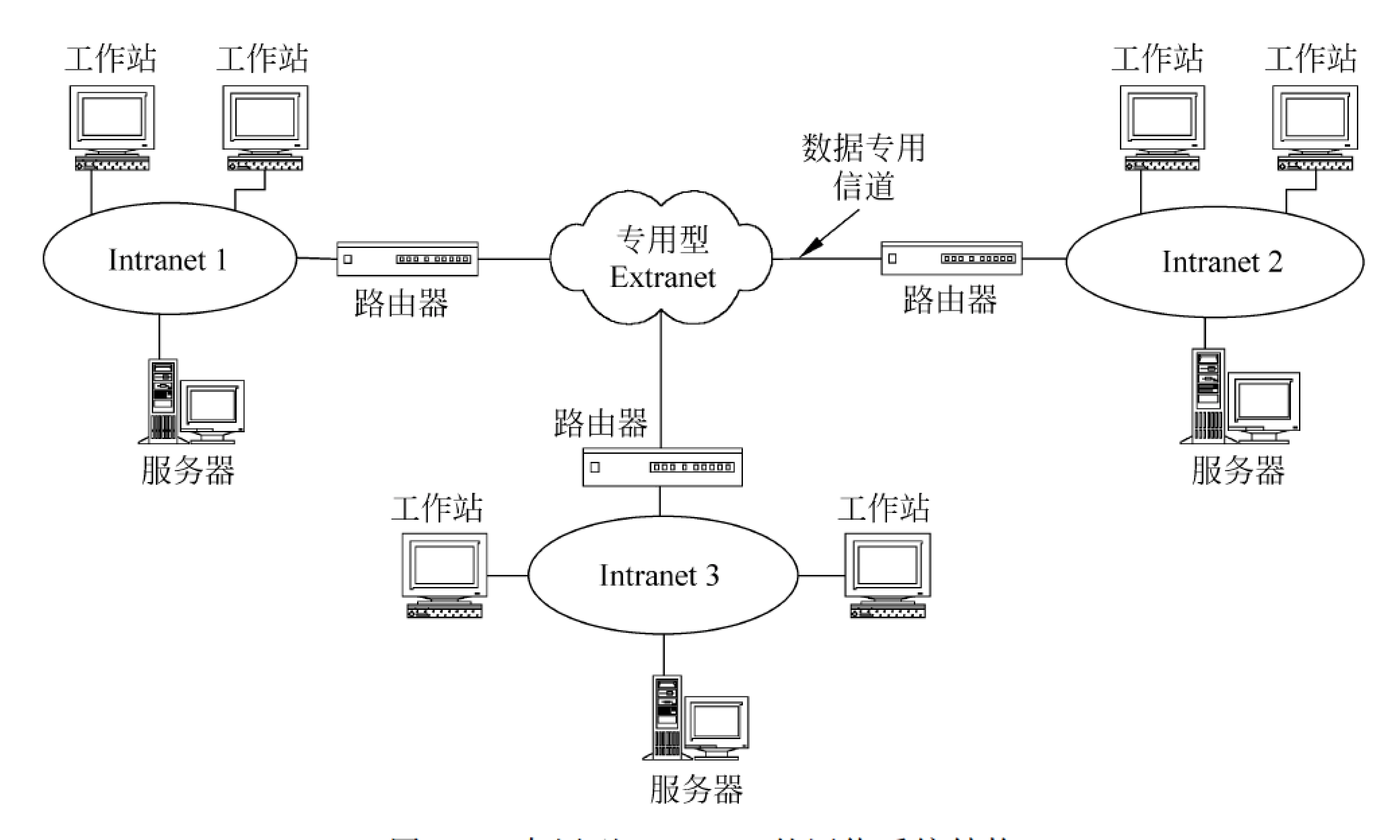


图 3-4　专用型 Extranet 的网络系统结构

所谓虚拟专用网是指利用公用网的资源为用户构建的外部专用网，常见的公用网有 DDN、X.25 和 ISDN 等。使用虚拟专用网构建 Extranet 是解决其安全问题的一种行之有效的方法。

(2) 专门建立主干网的方式

构建 Extranet 的另一种方法是专门建立主干网来连接各相关企业的 Intranet 以及 Internet 的客户。一般使用路由器和访问服务器进行互联，其中，路由器用来连接 Internet，访问服务器用来连接远程访问的电话线用户。

4. Extranet 网络的安全策略

解决 Extranet 网络的安全问题有两种方法:其一,通过构建 VPN 的方式,使用数据加密技术和网络隧道技术;其二,每个 Intranet 采用基于防火墙的防御措施,例如,可以采用外部防火墙加中间服务器的方法防止来自外部的非法存取等。

5. Extranet 使用的软件

Extranet 使用的软件与 Internet/Intranet 类似,这是因为这三者都是基于 TCP/IP 技术构建的。Extranet 使用的软件主要有 Web 服务器软件、Web 客户机软件和 Extranet 服务软件。

6. Extranet 与 Internet/Intranet 的关系

Extranet 使用的技术与 Internet/Intranet 一致,但它的范围介于两者之间。

从本质上说,Extranet 更像是一种思想和概念,它扩展和延伸了企业组织与管理的含义,而不仅仅是一种技术。Extranet 超越了企业本身,并由此带来了企业管理、企业经营、网络安全、信息保密和企业间的协作关系等许多问题。因此,实现 Extranet 时,不仅涉及到技术问题,更重要的是涉及到企业管理理念、经营观念、组织结构、企业战略等多种管理层次的问题,这既是 Extranet 的难点,也是 Extranet 的未来发展的必然趋势。

企业之间使用 Extranet 技术后,可以极大地扩展 Intranet 的功能,为企业建立更加广泛的商务联系,促进网络商业贸易的发展,开展区域或全球经济合作和科学研究等。由于 Extranet 正处在发展和起步阶段,其真正发展起来尚需一段时间,因此,本书将 Intranet 作为重点,而对于 Extranet 就不再多作介绍。

习题

(1) 什么是 Internet? 什么是 Intranet? 它们之间有哪些相同和不同?
(2) 什么是 Web?
(3) 什么是主页、网页和超级链接? 它们之间的联系和区别又是什么?
(4) 什么是超文本、超级链接和超媒体? 它们之间的联系和区别又是什么?
(5) 超文本传输协议 HTTP 在什么场合使用?
(6) 请解释标准的 URL“http://www.sohu.com/index.html”的含义。
(7) 统一资源定位符有何用处? 它包含几个部分,各有什么含义?
(8) 什么是 IP 地址? 什么是 DN? 什么是 DNS? 它们之间的关系是什么?
(9) Intranet 的特点是什么? Intranet 的核心技术又是什么?
(10) 试比较 Internet 和 Intranet 的联系与区别,并说明它们的中文名称。
(11) 试比较局域网和 Intranet 的联系与区别。
(12) 请画出 Intranet 的逻辑结构图。
(13) Intranet 的核心技术是什么? 它的三个关键是什么?
(14) 什么是 Extranet? 它是如何定义的?
(15) 什么是 VPN? 它的中文名称是什么?

(16) Extranet 网络有几种类型？各有什么特点？
(17) 请画出开放式 Extranet 的网络结构图。
(18) Extranet 网络使用的主要软件有几种？
(19) Extranet 中的安全策略有几种？
(20) Internet、Intranet 和 Extranet 的联系与区别。

实训题目

使用 Internet Explorer 工具，理解和熟悉 WWW 上的信息浏览与查询。

(1) 实训条件

具有共享接入 Internet 的实验环境。

① 安装有 Windows 98/Me 操作系统的计算机。

② 具有共享连入 Internet 的环境，或者具有模拟接入 Internet 的环境。

③ 操作系统中安装了 IE 浏览器，或者是其他浏览器软件，例如 Netscape Communicator。

(2) 实训目标

通过实验掌握 Windows 95/98 中 IE 软件的安装与配置，熟悉搜索 Web 站点的方法、IE 浏览器的菜单界面和按钮的功能及其使用技巧。

(3) 实训内容

① 掌握 Internet 上常用浏览器(IE 或 Netscape)的安装与使用方法；

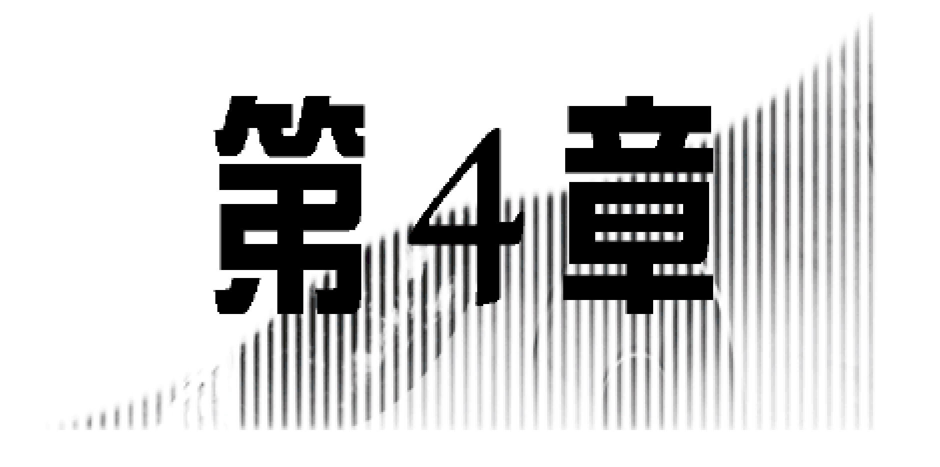
② 掌握 URL 地址的含义和使用，使用 IP 地址和 DN 进行站点的搜索；

③ 掌握从 Web 上查找和下载信息的方法；

④ 掌握查看历史记录的方法；

⑤ 掌握使用收藏夹的方法；

⑥ 掌握浏览器首页的设置方法。



第4章 网络系统集成

本章主要介绍网络系统集成的基本概念。通过本章的学习,应当掌握网络系统集成的基本概念,使用的方法和原则,以及网络规划、网络系统设计和实施过程的具体内容及要求。

主要内容:

- 网络系统集成的基本概念;
- 网络系统集成的目标、方法和工作内容;
- 网络规划和设计的过程;
- 网络规划方案的制定;
- 网络系统的总体设计和实施计划。

4.1 网络系统集成概述

随着经济全球化和信息社会化的深入发展,网络技术日新月异,网络的规模日益庞大。从局域网、广域网、Intranet、Extranet 到 Internet,网络系统逐步从封闭走向开放。这一切使得人们在面对着迅猛发展的网络技术的同时,还面临着对传统网络建设思想和规则的挑战。在计算机网络信息化的今天,网络管理的模式已不应再是传统、单一的手工管理的作业方式,而需要采用从复杂的总体对象出发的现代管理作业方式。这就是从“系统”的角度出发,运用系统化的方法进行管理和建设网络。

4.1.1 网络系统集成的基本概念

网络系统集成就是指根据用户的需求,优选各种网络技术和产品,使整个系统能够协调工作并发挥最佳效益,从达到整体性能优化的目的。

1. 系统的概念

系统就是由同一个目标联系起来的、相互影响的有机体。如一个科研机构、一个研究项目的开发计划、一个公司的运营管理机构等,均可以被看作为一个系统。一个公司的管理系统是由该公司的经营、财务、人事和销售等多个部门组成的,这些部门组成了一个相

互制约、相互联系的有机整体。公司的管理系统是处于运动状态的，其目的是为了完成公司的经营计划。由此可见，系统具有3个必要的条件，即系统组成的目的、系统的功能和实现系统功能的机构。

2. 系统集成的定义

系统集成就是通过系列的工作方法，使得一个系统的各个部分之间能够有机和协调地工作，从而可以发挥整体的效能、达到整体的优化、实现整体的功能。

3. 网络系统集成的目的

在建设网络系统时，人们应当如何根据自身的需求进行规划和设计，又应当如何考虑和开发网络上的应用系统，并取得网络应带来的经济效益等多种问题，已成为网络建设中急需解决的问题。简单地说，选择何种网络系统、拓扑结构、服务器、工作站、网络操作系统和信息系统的软件，由哪些厂商提供网络系统的软硬件支持等问题，已经不再是多个简单部件、简单过程的组合，而是一个集技术和管理于一体的网络系统集成的问题。网络系统的集成问题已经明确地提出，并成为一项不容忽视的工作。

网络系统集成的目的就是在达到用户目标、满足用户需求的前提下，优化选择各种先进的技术和产品，将各个分离的子系统（或部分）连接成为一个完整、可靠、经济和有效的系统的实施过程。但应注意，集成绝非只是简单地进行设备或过程的组合，而是经过选择先进的产品和技术，完成系统软、硬件配置和系统功能的整个实施过程，从而达到整体优化的目的。

4. 网络系统集成的内容

网络系统集成不仅涉及到技术问题，还涉及到人文、地理、心理、艺术和管理等问题，其主要内容包括以下几个方面：

① 硬件集成　是指使用各种硬件设备将各个子系统连接起来，以达到或超过系统设计的技术性能指标。例如，交换机制造商可以利用集线器、交换机、路由器、Internet接口等多种硬件设备进行硬件集成，为用户创造出一种更加高效和便于管理的网络工作环境。

② 软件集成　是指为了特定的应用环境而架构的工作平台。简单地说，就是为了提高工作效率而创造的环境，如为某一特定环境提供的不同软件连接的接口。例如，微软为了使用户可以更方便地访问Internet，将Windows操作系统与IE浏览器集成到一起，使得微软的桌面系统的功能更加强大。

③ 网络技术集成　开始时主要指计算机局域网，随着网络技术的应用和发展，又相继出现了智能大厦系统集成和智能小区系统集成。例如，局域网系统集成，主要包括网络互联设备、传输介质、布线系统、服务平台和网络操作系统等内容。

④ 数据和信息集成　数据与信息的集成建立在硬件集成和软件集成的基础之上，是网络系统集成的核心，通常需要解决以下问题：合理规划数据和信息；减少数据冗余程度；更有效地实现信息共享；确保数据和信息的安全和保密性。

⑤ 技术与管理集成　企业和公司等单位的核心问题是经济效益，因此，如何使各部门协调一致地工作，实现市场销售、产品生产和管理的高效运转，是网络系统集成的重要内容。

⑥ 人员与组织机构的集成　这是系统集成的最高境界，因此，如何提高每个员工和

各个组织机构的工作效率，并通过系统的集成来促进企业的管理、提高管理效率，是系统集成面临的重大挑战，是值得很好地研究和解决的问题。

4.1.2 网络系统集成的目标、方法和工作内容

网络系统集成是一个复杂的系统工程，它包含了系统的目标、方法和工作内容3个部分，其工作流程如图4-1所示。有关概念简述如下：

1. 目标

任何工作都有自身的目标，网络系统集成的目标有两个：

① 用户目标　是指用户投入了人力、物力和财力建立的网络所能够达到的、有关用户需求的明确要求。例如，网络能够提供Internet浏览和邮件服务等。

② 系统集成目标　是指根据用户目标所提出的目标保证。例如，根据上述的用户目标，系统中应有WWW服务子系统和邮件服务子系统。

用户目标侧重于要求，系统集成目标侧重于能否实现要求的保证。两者之间既有相同之处，又有不同的侧重点。在系统集成的过程中，要遵循"一致性原则"，即首先明确用户目标和系统目标，若遇不一致时，需要进行反复协调，最终达成一致，即系统集成完成的目标一定是用户提出的目标，因为，用户将依据系统集成的目标验收最终的网络系统。

网络系统集成的最终目的是提供满足用户需求的最佳方案，即保证在实施网络规划、网络设计中的各种复杂技术可以相互协调。切实保证网络的连接性、互操作性、网络的可管理性和网络的安全性，并且可以保证在网络环境下遇到问题时，有解决的方案和措施。

2. 工作方法

网络系统集成的任务并非简单的硬件和软件的组合，因此，采用何种开发方法来确定网络的建设是非常重要的。可选择的开发方法有独立开发、联合开发和委托开发3种，究竟选择哪一种，应当视部门的具体情况而定。无论使用哪种方法，在网络建设中都必须采用先进的理论指导、完善的技术保证和工程化的管理手段来确保系统的顺利实施。下面

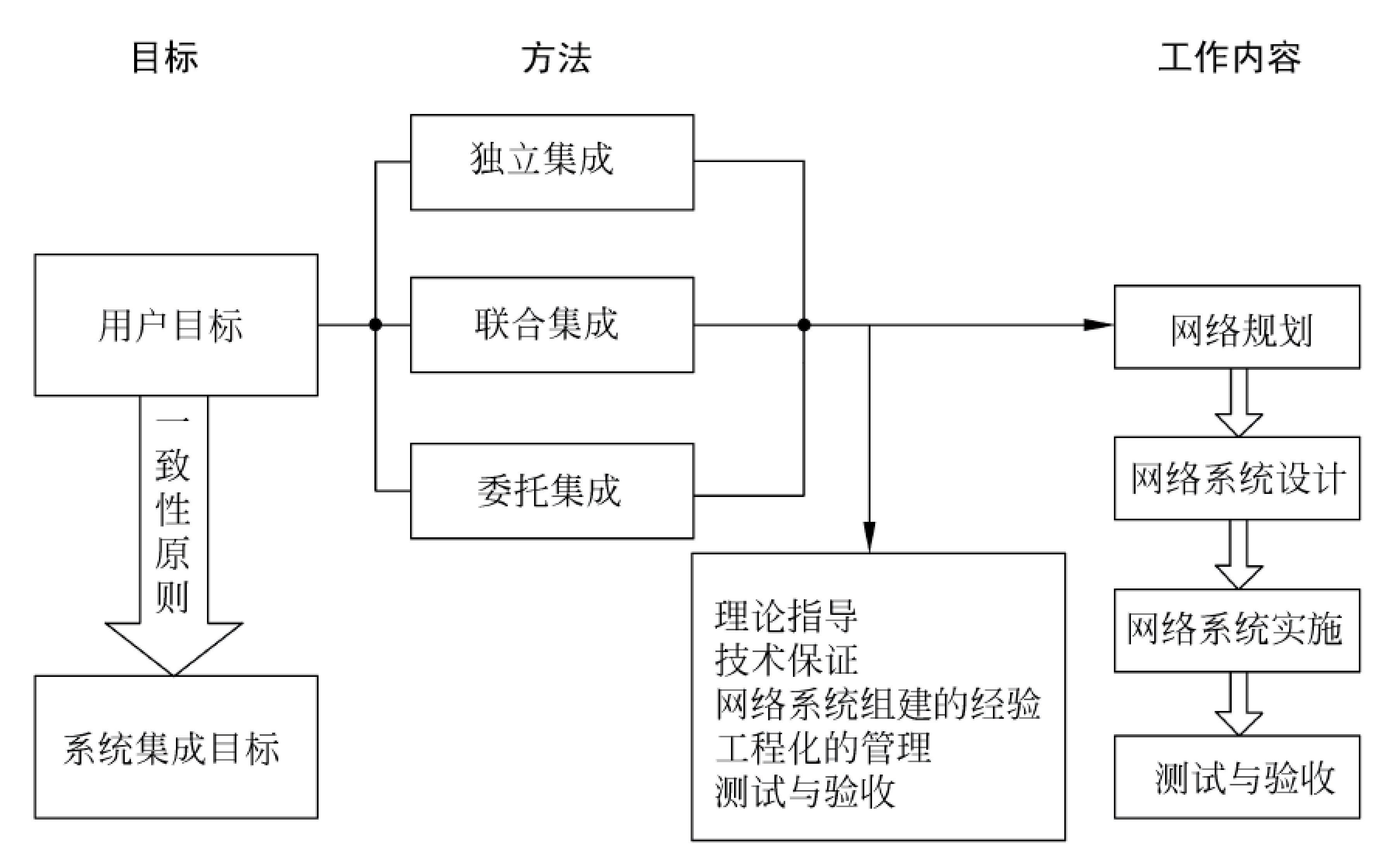


图4-1　网络系统集成工作流程示意图

具体介绍一下这 3 种方法。

（1）独立集成

独立集成即从网络规划、设计到网络系统的实施等过程，完全由自己的力量解决。这种方法对大多数单位并不适用。因为，只有当实施方案的单位或部门在信息管理技术、计算机网络技术、数据通信技术等各个方面都具有较强的实力，有着丰富的网络系统集成经验，并能够解决网络建设过程中出现的管理和技术问题时，才适合采用独立集成的方法。

（2）联合集成

联合集成即联合两个以上的部门和单位完成网络系统集成的任务。此方法适用于本单位不具备网络系统集成的全面规划人员，或者是缺少某一方面的技术人才，对于实施大规模的网络建设确有困难的场合。为了完成任务，只有联合部分关键性人才，或者将系统集成中的部分任务交给有网络开发经验的机构完成，才能弥补自身技术力量的不足。在选择这种方法时，应当着重注意分清双方的任务和职责范围，以避免出现问题时，由于双方职责不清而互相推诿、影响工作。

（3）委托集成

委托集成即委托网络系统集成商进行系统集成。网络系统的建设是一项复杂的、专门的技术性工作，大多数只使用网络系统的单位通常不具备完成这种工程的技术力量，而且也不具备应付网络系统集成过程中所出现的各种问题的能力，这时只能选择委托集成的方法。

在以上 3 种方法中，用户应当根据自身的实际情况进行选择。在系统集成任务开始以后，为了确保网络集成达到用户目标和系统集成目标，应当从以下几个方面进行考虑和监督：

- 确保采用先进、实用、可靠和安全的理论作为技术指导；
- 选择熟悉网络技术、设备、性能和软硬件技术的人员是网络集成的技术保证；
- 应当注意使用具有建立网络系统经验和组建同类网络经验的部门进行系统集成的开发；
- 工程管理人员应当按照工程化的管理标准来管理整个的工作过程，其中包括制定计划、设计方案、制定工作日程、协调工程进度等具体实施内容；
- 网络使用单位应当严格按照系统集成所制定的网络系统测试项目和验收的标准进行系统验收。

3. 网络系统集成的工作内容

在网络系统的集成过程中，主要的工作内容包括以下几个方面：

（1）网络规划

网络规划的目的是为即将建立的网络提出完整的设想和方案。其中，应当包括网络系统的可行性研究的计划、需求分析、网络中硬件设备和软件的选择、网络系统的选择、网络结构设计、投资预算和建立规范化的网络技术文档等内容。

（2）网络系统设计

在网络规划的前提下，网络系统设计的任务包括：网络拓扑结构的设计、网络服务器和工作站的选型、网络工程的结构化布线、网络操作系统的集成、应用软件的集成与开发

等。此部分工作的技术性要求很强，因此，需要从事网络设计的专门技术人员完成。

(3) 网络系统的实施

网络系统的实施包括采购、硬件设备的验收、安装、配置、集成、系统测试，以及按照系统设计实现网络系统的连接，直至所有设备和系统的正常运行，并负责最终的培训和系统维护。而严格的工程化管理是保证系统顺利实施的前提条件。

(4) 网络系统的测试与验收

应根据系统的目标和网络设计的内容，来制定具体的网络测试指标和详细的验收标准。

以上简单地介绍了网络系统集成的基本概念、目标、方法和工作内容，下面将针对其中的重点作详细介绍。

4.2 网络的规划与设计方法

网络的规划与建设是一项复杂的工作，它具有涉及面广、专业技术知识要求高和管理复杂等特点，因此，需要使用一整套系统工程的规划与设计方法。本节将简要介绍网络规划与设计的原则及考虑因素。

4.2.1 网络规划和设计的过程

1. 网络系统规划与设计的一般步骤

(1) 需求分析

任何网络的建设，需求分析是必不可少的，它的主要任务是确定建网的目的、所要完成的工作，以及完成的方法和步骤。需求分析应当包括以下几个方面：

① 可行性研究。

② 环境要求。

③ 设备配置。

④ 功能需求。

⑤ 成本和效益分析。

⑥ 风险投资。

⑦ 用户目标。

⑧ 网络系统目标。

(2) 网络规划

① 技术性论证。

② 网络先进性、实用性和可靠性的设想与规划。

③ 总体规划。

④ 难点估计。

⑤ 经费预算。

⑥ 文档规范。

(3) 网络总体设计

① 网络系统模式的设计。

② 网络拓扑结构的设计。

③ 网络节点规模的设计。

④ 网络操作系统的选择。

⑤ 结构化布线系统的设计。

⑥ 主要数据库管理系统的设计。

⑦ 编制总体设计说明书。

⑧ 网络系统软件、硬件的配置清单。

进行一个真实网络系统的总体设计时,应当根据网络规模的实际情况来酌情选择、灵活处理。例如,当所设计的网络规模很大时,组网所采用的应用技术就会较多,因此,必须严格遵循统一的步骤,精心设计,否则很容易出现意想不到的差错。如果所设计的网络规模较小,技术单一,那么对于上述步骤就应当有所取舍,以求简化工作过程。

2. 网络系统规划与设计的基本原则

网络规划的目的是为要建立的网络提出一套或多套规划和设想的方案。网络设计的目的是在网络规划的基础上进行更深入的分析和论证,进而实施规划。规划与设计相辅相成,两者缺一不可。

在设计院,通常是先由规划所对工程项目进行规划设计,再由工程设计所做出详细的设计和实施方案。前期规划只提出规划草案,后期才提供具体的设计、施工报告,这就是所谓的先规划,后设计,最后施工的工作模式。为了使整个网络系统的建设更合理、更经济、性能更好,设计者应该遵循以下原则:

(1) 认真做好需求分析

需求分析应当本着实事求是的原则,所提的要求应当有理有据,其目的在于为网络规划和设计奠定扎实的基础。在需求分析之前,应当由用户首先提出需求报告,规划人员再在此基础上开始进行规划和设计。但是,对大多数用户来讲,由于他们本身对网络的功能、技术和有关业务的了解往往不够深入,因此,这项工作并不是一件容易的事,他们提供的需求报告也往往是不太符合实际的和不理想的。

(2) 确保网络具有先进、可靠、安全和实用等网络性能

在进行网络规划和设计时,要充分保证所设计的网络具有较好的先进性、可靠性、安全性和实用性等综合性能。例如,服务器、主干网交换机和网络干线等网络的核心环节应选择先进、可靠和高质量的产品,否则会降低网络的可靠性。因为,一旦这些关键设备出现问题就会造成网络的瘫痪。下面将详细讨论这几项性能:

① 先进性　网络系统的先进性是网络设计人员首先需要考虑的问题,只有设计先进的网络,才能使系统达到更高的技术指标,具有更强的功能和良好的使用性能。例如,对于网络主服务器,在经济条件许可的情况下,应尽可能选择性能良好、质量高和可靠性强的专业厂家的服务器,而不应采用普通计算机。

② 可靠性和实用性　设计时,新的技术在实用性和可靠性方面尚未经过实践的考验,因此,不能片面追求先进性,而不去注意新技术可能带来的风险性和不可靠性。设计

人员应当根据实际情况，综合考虑这三个性能。

③ 安全性　随着网络上各种安全问题的出现，对网络安全性能的要求日益增加。因此，对所设计和组建的网络的安全性必须具有明确的措施和指标要求。

（3）统一建网模式，确定网络总体结构

在确定网络总体结构时，应统一建网模式，保证网络功能的完善。设计时，应对主干网、本地网的衔接，网络技术的相互匹配，数据传输和网络操作系统的选择等多种因素进行充分的论证。

（4）确保网络具有良好的开放性和可扩充性

在设计时，应充分考虑到网络的发展和网络规模的扩大，因此，应采用易扩展的网络拓扑结构，选择有良好扩充性的网络关键设备。

（5）确保网络具有良好的安全性和保密性

对网络中使用的安全、保密技术和指标要求将在后续章节中作详细的介绍。

（6）网络应具有良好的可维护性

综上所述，网络的规划与设计是一项复杂的技术性工作。由于各单位对网络的需求不同，采用的网络技术不同，因此，达到的目标也就不同。若想完成一个高水平的网络规划和设计，在设计之前，应当成立有领导及专门技术人员参加的规划领导班子，以求统一步骤、精心策划。设计和规划人员，除了对业务熟悉和目标明确之外，还应对网络的软件、硬件和信息管理具有相当的知识，并具有组网工程方面的全面控制能力和设计经验，这些都是组网成败的关键所在。

4.2.2　网络规划方案的制定

完成需求分析之后，应制定网络规划方案，其主要任务是在需求分析论证的基础上，将用户提出的问题和要求，用计算机网络方面的术语描述出来，经过技术上的分析，提出包含以下内容的网络系统方案：

- 对需求分析的技术性论证；
- 网络系统对先进性、实用性和可靠性方面的设想；
- 网络系统的总体规划；
- 网络系统的难点、关键性的估计；
- 网络经费预算；
- 网络规划文档的编制。

1. 需求分析的技术性论证

需求分析只是一个在用户需求基础上，由部分系统人员做出的粗略的调查报告，它只能反映用户的需求和目标，是网络系统的宏观目标。因此，不能以此方案作为网络的规划方案。因为，从网络技术人员的角度看，用户的某些需求可能是不切实际的，在目前的技术条件下，有些可能是实现不了的。那么，重要的任务就是对用户的问题做出技术分析，从而找到用网络系统解决这些问题的途径。解决这个问题的方法有以下两种：

① 当需求分析及用户目标做得很详细和充分时，技术人员也应逐条论证，并做出明确的技术实施保证。

② 当需求分析及用户目标做得不够充分，或者是由一些不熟悉计算机和网络技术的用户提出的需求报告时，双方的沟通将是非常重要的和必不可少的。否则，在网络建设工程的后期将会出现许多不必要的麻烦。沟通的方法可以采用交互式的问答方式，设计和规划人员应当就用户提出的问题做出尽可能多的解释，以求用户充分地理解设计人员所使用的技术方案的特点。例如，当用户担心所设计的网络是否能够用来可靠传输多媒体为主的数据时，设计人员可以建议采用 FDDI（光纤分布数据接口）网络、ATM 网或千兆以太网等，并应当分别说明各自的特点和需用的资金。

总之，上述工作的根本目的在于，使得网络规划和设计人员能够充分、准确和全面地掌握用户的需求，使用户了解可能采用的方案和投资情况，为日后的网络建设工作打好基础。

2. 网络性能的设计

网络系统的规划和设计应当确保所设计的网络具有良好的性能，因此，应当包括先进性、实用性、安全可靠性、开放性与可扩充性等性能方面的设计与分析。

3. 网络系统的总体规划

在进行网络系统的总体规划时，规划人员应当着重考虑以下 4 个方面的问题。

(1) 网络的分布

网络的分布主要包括以下内容：

① 网络用户的数量。

② 网络用户的地理位置。

③ 任意两用户之间的最大距离。

④ 明确用户之间的联系与相互依赖关系，进行用户关系分类。

⑤ 用户地理位置分组，主要指将处于同一建筑内或同一楼层内的用户分组排列。

⑥ 明确在所建网络区域范围内的所有建网的要求和限制。

⑦ 弄清有无直接可利用的通信设备及线路。

(2) 网络的基本设备和类型

① 确定网络用户工作站（计算机）的总量，应当分别指出可以在网络上同时运行的工作站数目和需要新增加的计算机数目。

② 确定网络用户工作站（计算机）的类型，即它们的型号和具体配置。

③ 确定网络服务器的数量，应当指出所需服务器的数量和类型，例如，指明采用的是专用服务器还是一般的高档微机，以及这些服务器的具体配置要求。

④ 确定网络共享设备的数量和类型，应确定常用的交换机、集线器、路由器和通信设备等原有的数量和需要增添的数量，还应指出这些设备的具体型号和特定要求。例如，所采用的路由器要求 WAN 口支持 128Kb/s 的 ISDN 基本速率，LAN 口为 RJ45 端口等。

⑤ 网络用户所用的其他设备，例如，需要配备高速的网络激光打印机等。

(3) 网络的基本规模

① 所建网络是局域网、广域网、Intranet，还是需要与其他合作伙伴相连的 Extranet。

② 网络互联设备的数量和型号。

(4) 网络的基本功能和服务项目

应当根据用户的实际需求确定网络中应具备的服务子系统。

① 用户设备之间的逻辑连接。

② 数据库系统和应用软件系统。例如，建立能够在 WWW 浏览器上浏览的数据库。

③ WWW 服务。例如，Web 方式的信息管理系统。

④ 文件传输。例如配备 FTP 服务器提供文件传输和共享服务。

⑤ 电子邮件服务、网管系统和计费系统等。例如，提供在局域网和 Internet 中传送电子邮件的功能。

⑥ 网络互联系统。例如，提供 100 人同时浏览 Internet 信息资源的能力。

⑦ 虚拟网络系统。

⑧ 防火墙系统。例如，应保证内网数据资源的安全。

4. 网络系统难点预测

在进行网络设计时，要充分估计到可能出现的问题。可预测到的网络系统难点和关键性的问题归纳起来有以下几类：

(1) 网络设备之间的不匹配

在网络工程的实施过程中，由于产品设备的厂家和标准不同而引发的问题有很多，尤其是在采用新技术、新产品的过程中，由于技术和施工人员对新的设备和技术的指标及性能了解不够透彻，将会导致实施过程中的许多困难。

(2) 网络拓扑结构不合理

当网络拓扑结构的设计不合理时，会造成数据传输中的瓶颈，引起严重的阻塞问题。

(3) 线路连接故障

由于布线和施工的问题，而引发的线路不通、线路时好时坏的现象，将可能导致网络运行的异常。

(4) 网络操作系统选择不当

当网络操作系统选择得不恰当时，会使得用户的一些必要的应用软件无法运行。在组网中，除了上述问题外，还会有许多其他类型的问题。因此，在设计时，网络设计人员应当根据以往的实际经验，在关键问题上有充分的思想和物质准备；在施工中，应当切实把握好每一步的质量关，才能杜绝常见的问题，使得工程得以顺利进行。

5. 网络经费预算

网络系统的经费预算是网络规划中不可缺少的部分，也是各主管部门所关注的主要项目。网络系统投入的经费，应当包括原始投入和维持费用两个部分，具体内容包含以下几个方面：

(1) 硬件设备投资费用

硬件设备的投资费用主要包括：网络服务器、工作站、交换机、集线器、路由器、网卡、布线设备及材料和辅助设备等。

(2) 软件投资费用

软件投资的费用主要包括：软件购置和开发设计费用两项。前期需购置的常用软件有：网络系统软件(工作站系统软件和网络操作系统等)、数据库系统、网络工具、网络管理和网络互联软件等。而应用软件的开发费主要发生在系统建设的后期。

(3) 安装调试费用

安装调试费用主要包括:网络集成、设备安装和布线等费用。

(4) 培训和服务费用

培训和服务费用主要指人才的培训费用,其中包括网络系统管理培训、使用培训和网络应用软件培训等几个方面的培训费用。

(5) 维持、运行和维护费用

网络运行之后,为了保证网络系统的正常运行,必须考虑到系统的维持、运行和维护费用。例如 Internet 运行和维持费用、新增网络系统维护人员所需的人工费用、常用耗材和自然损耗等多种费用。

在进行网络规划时,对于上述这些费用,应当本着实事求是的原则,对所需的费用进行逐一审核和落实,并对市场的不可预测的情况留有充分余地。为了避免今后的麻烦,通常使用工程造价的 10%~15%的金额作为未知因素的预测支出。经过以上各部分的详细预算之后,应当列出网络预算的清单,参见表 4-1。

表 4-1　网络经费预算清单

分类	项目		型号	数量	单价	金额
硬件设备投资	计算机设备	服务器				
		工作站				
	网络共享设备	集线器				
		交换机				
		路由器				
	网络配件	UTP 双绞线				
		光纤				
		……				
	……	……				
软件投资	网络系统软件	Windows NT Server				
		Windows 98/2000				
	数据库	SQL Server				
	……					
安装调试费用	设备安装					
	……					
培训和服务费用	使用培训					
	……					
运行和维护费用	Internet 使用和运行费用					
	……					
总计						

6. 网络规划技术文档的编写规范

在网络规划的每一个阶段中，都会产生一些很重要的技术性文档，这些文档将对网络的设计和网络工程的实施起着重要的指导性作用。对于网络规划文档的总体要求是简明扼要、全面、准确和翔实。因此，技术文档的规范化是十分重要的。由于网络系统的规模、技术要求和系统目标各不相同，所以网络规划文档的格式也并非千篇一律。但是，就某一类网络规划的技术文档而言，却应该大体一致。一般地，在进行了用户需求的调查之后，将生成两个建网的技术报告，即"可行性研究报告"和"需求分析报告"，这两个报告是网络建设的指导性的文件。因此，需要与用户反复讨论后，进行编写。下面给出这两个文档的主要内容和大体的书写格式，以供读者参考。

① 网络系统名称。

② 建网的必要性说明。

③ 需求分析。包括用户目标、系统目标和需求分析报告。

④ 网络系统功能性说明。

⑤ 网络性能的简要说明。

⑥ 网络的规划与实施计划。包括技术性论证、总体规划方案和网络经费预算。例如，硬件和软件的建设费用、系统的开发费用、资源使用计划、开发进度安排和人员的组织等。

⑦ 网络的效益分析。由于行业、单位、部门的不同，建网的效益对用户来说是潜在的而不是即时兑现的，因此，很难做出估计。通常采用估算的方法进行经济效益分析。例如，有材料表明，对于建立管理信息系统（MIS）网络的企业单位而言，其建网的效益可使用下面的公式进行计算。

$$效益=企业的年产值\times 8\%$$

在网络的规划设计中，设计方案往往不止一个。一般地，考虑到各种主观和客观的因素，例如，根据领导对网络必要性的认知程度，以及可能使用的经费等，可以做出至少两套以上的方案，以供用户选择，每个方案的性能指标和侧重点应有所不同。

7. 网络规划设计方案选择的误区

在进行方案的规划和设计时，应注意避免下面的几种状况：

① 只有硬件的投入，而无软件开发。这表现在硬件投资时，不惜资金，但应用软件的开发投资却很贫乏，因此，不能真正发挥园区网络的作用。

② 具有了网络的外形，却无网络的实质。这表现在仅仅把电脑连接起来，就美其名曰建成了"校园网"，但其实质是既未实现网络办公，也未实现网络的应用开发，甚至连网络的基本功也未能利用。

③ 有网络建设，无网络的科学管理。这表现在，资金已经投入，网络管理人员已经到位，但是没有制定相应的制度，也没有网络的规范。

④ 网络规划的配置不合理。这种现象有两个极端：第一种，追高求新，配置的设备功能很多，但是闲置的也很多；第二种，一味求廉价，结果是配置低到功能不够用，几个月内就得升级。

4.2.3 网络系统的总体设计和实施计划

网络的规划只是为网络系统提出整体设想或方案，它并未给出网络性能的具体指标和实现方法。因此，在网络规划之后，还要做出具体的网络总体设计。

在网络总体设计阶段中，设计人员应当对各种技术规范、系统的性能、实施与施工的技术细则等做出具体的设计方案。网络总体设计的内容与规划设计的内容相仿，只是更加具体。

网络系统的总体设计和实施计划的主要内容应当包括以下几个方面：

① 网络结构的确定；

② 网络拓扑结构的选型；

③ 网络中主要硬件设备的选型；

④ 网络操作系统的选择与确定；

⑤ 结构化布线工程的设计；

⑥ 信息管理系统的设计；

⑦ 总体设计说明书的生成；

⑧ 网络软件和硬件的配置清单。

网络建设的实施计划除了包括上述的具体工程计划之外，还应当包括：网络的硬件建设和软件建设的费用清单、系统的开发费用，资源的使用计划、开发进度计划和人员的组织计划。

习题

(1) 什么是系统集成？它包括哪 3 个基本条件？

(2) 网络系统集成的定义和目的是什么？

(3) 什么是网络系统集成？其内容包括哪些部分？

(4) 为什么说网络系统集成是一项不容忽视的工作？

(5) 网络系统规划与设计的基本原则是什么？

(6) 网络性能设计的基本原则是什么？

(7) 在进行成本和效益分析时，应从哪些方面考虑？

(8) 常用的网络系统模式有哪几种？各有什么特点？其中 C/S 和 B/S 有何区别与联系？

(9) 网络系统总体规划应考虑的问题有哪些？

(10) 网络系统可能出现的难点和关键性问题有哪些？

(11) 根据网络规划文档的规范，网络的规划文档应包括什么内容？

(12) 网络系统的总体设计包括哪些内容？

(13) 网络经费预算包括哪几部分？

(14) 网络系统规划与设计的主要步骤有哪几步？

实训题目

规划一个分布在3栋楼中的中型企业的局域网络。

(1) 实训条件

某公司分布在1号楼、2号楼和3号楼中。

① 1号楼　三层建筑,为该公司的主要办公楼,内有财务部、销售部、人事行政部和服务部。计算机的总量在30台左右,其中需要连入Internet的计算机大约有15台。

② 2号楼　二层建筑,为该公司的研发楼,内有研发部。计算机的总量为20台,全部需要连入Internet。

③ 3号楼　二层建筑,为该公司的生产楼。计算机的总量为2台,全部需要连入Internet。

(2) 实训目标

建立该公司的局域网Intranet方式的管理应用系统。写出网络规划设计的技术文档。



系统集成在 Intranet 中的应用

通过本章的学习，应该掌握中小型 Intranet 系统的具体规划、设计与实施过程，从而进一步理解和掌握网络系统集成有关的思想、方法、技术和具体工作内容，并深入理解网络管理员在网络管理初期中的工作内容。

主要内容：

- Intranet 的网络结构与建设方法；
- Intranet 的规划、设计和架设；
- Intranet 中网络操作系统的选择与确定；
- Intranet 中的网络服务子系统；
- Intranet 的实施；
- 使用 Windows NT 管理 Intranet 的目标和内容。

5.1 Intranet 的网络规划、设计与建设

前面已经介绍了网络集成的有关理论、方法和内容。本节以中小型 Intranet 为例，介绍网络规划与设计中应考虑的系统功能、网络安全和应用等问题。

网络系统的建设是一项系统工程，从网络的规划、设计到实施，每个步骤都很重要，Intranet 也不例外，由于其应用的伸缩性很强，规划和设计信息网络时，不要追求一步到位，应当根据企业网的实际情况由小到大，逐步建立起来。例如，可以先从企业的某个部门开始，根据信息需求量的增加而逐步增加网络中的内容，直至覆盖到整个企业的 Intranet。

本章所规划的对象是一个中小型 Intranet，在实际系统集成中，对此类对象通常作简化处理，即将规划和设计的过程合并进行。

5.1.1 Intranet 的规划过程

网络规划就是根据用户的具体应用要求，遵循最佳性能价格比的基本原则，在众多新技术、新产品和方案中为用户做出正确的抉择，使用户得到一个最佳的计算机网络系统。

1. 可行性研究

任何一个项目的规划过程都应当包括可行性研究。对于建设企业的 Intranet 来说,也不例外。如前所述,这个可行性研究报告应当包括经济评估和技术评估两个主要部分。

2. Intranet 的环境评估

建立 Intranet 之前,必须对企业实施 Intranet 的环境进行评估。该项评估包括企业各级领导和员工对建立 Intranet 的认识程度和态度的状况等。如果这些环境因素不能满足实施 Intranet 的要求,则应改善之后再进行,否则很难完成建立 Intranet 的任务。如果环境符合要求,也应当建立一个由高层领导、技术人员和经营人员组成的 Intranet 建设领导小组。

3. 规划设计 Intranet 的原则

如前所述,在进行较大规模的 Intranet 的规划设计时,应当包括分析、模块化与集成等多个复杂的过程。

对于中小型的 Intranet 来说,由于其具有规模较小、功能简单等特点,在实际工程中通常将其网络的规划与设计合并简化为一个整体的过程。在这个过程中应当遵循如下几个基本原则:

① 应当充分分析用户的需求,最大限度地满足网络中客户的要求。

② 整个网络应当具有良好的性能价格比。网络的设计不但应当兼顾和考虑原有的软硬件资源,还应当尽可能地注意到网络设备具有更新快、技术新的特点,使得所设计的网络能够尽可能地保持较长的生命周期。

③ 应当兼顾实用性和先进性。设计时应当注重实效,紧密结合实际的需要,除了考虑采用先进的技术设备之外,还要注意所选的设备是否具有技术成熟、实用性好和市场的占有份额大等特点。

④ 具有较好的开放性和扩充性。在设计网络时,网络系统应该具有良好的开放性和可扩充性,以保证网络及其应用可以随时地延伸和扩充。

⑤ 保证系统的可靠性和稳定性。百年大计,质量第一。因此,在网络设计中,无论是网络的节点、布线工程、通信设备,还是网络的结构设计,均应以可靠性作为设计的出发点。

⑥ 有保障的系统安全性。尽可能地使用先进的防御技术,确保网络的安全性能。保证系统中各种数据对完整性、安全性的要求,并能够实现有效、安全的信息资源共享。

⑦ 系统应当具备较好的可维护性,不仅能够实现网络系统设计的合理性能,还应当配置有相应的检测设备和网络管理设施。

⑧ Intranet 应具有统一的界面,为用户提供方便、有效的使用窗口。

综上所述,应当尽量使所设计的 Intranet,在满足用户需要的基础上,具有先进性、高性能指标、高可靠性、良好的可扩充性和开放性、较高的安全性,以及可管理性能。

4. Intranet 应该达到的目标

企事业单位通过 Intranet 应实现下述目标:

① 对内可提供一个灵活、高效、宽松、可靠和理想的工作环境,以便信息交流、信息共享和企事业管理。真正实现企事业管理电子化、自动化和科学化,提高工作效率和竞

争力。

② 对外可全面展示企事业单位的形象，宣传和发布产品信息，保持与客户和伙伴的密切联系。

③ 可连接到 Internet，共享互联网上的丰富信息资源。

④ 企事业单位的领导在 Intranet 上可以实施各种先进的企业管理方法，进行企业的体制改革，确保企事业单位立于不败之地。

5. Intranet 应具备的基本功能

在规划和设计 Intranet 时，首先应当考虑到网络应该具有的功能，这也是人们建设 Intranet 的目的。下面简单地介绍一下 Intranet 所提供的基本网络服务。

① DNS(domain name server)服务　用于提供“域名解析”(也称为主机名/域名解析)，即提供 IP 地址和域名之间的转换服务。

② WWW(world wide web)服务　提供基于超文本方式的信息服务。利用 WWW 服务，不但可以实现信息资源的发布与浏览，还可以利用 WWW 服务器、客户端浏览器、文本信息检索服务(Gopher)和信息系统，实现企业内部信息的发布与信息资源的浏览。

③ E-mail(electronic mail)服务　提供基于计算机网络的电子邮件的交换服务。E-mail 不但可以在企业内部实现电子邮件的传递，还可以利用通信服务器和客户端软件，为企事业单位员工提供快捷、简单、费用低廉、可靠的 Internet 上的电子邮件服务，以及客户的远程通信。

④ FTP(file transfer protocol)服务　FTP 是 Internet 上应用最广的一种通信协议。使用 FTP 协议可以实现不同系统之间的文件传输。利用文件服务器、远程登录服务和远程登录服务等，可以实现文件资源的近程和远程共享，以及企业内部的文件和目录的查询与访问。

⑤ BBS(bulletin board system)服务　提供“电子公告板”的服务，同时也提供专题讨论区、聊天区、信件区和文件共享区等多种社区服务。

⑥ 企业内部打印共享　利用打印服务器组织与实现打印共享和打印管理。

⑦ 远程登录(Telnet)服务　通过 Telnet 服务，使得单位员工无论身在何处，均可访问内部网络中的信息资源。

⑧ 安全管理　与 Internet 相比，Intranet 的最大优势在于可以利用防火墙或其他安全技术实现网络的安全。

⑨ 其他网络服务　Intranet 通常还提供目录服务和网络管理等网络服务。

6. Intranet 设计和实施中涉及的主要技术

在 Intranet 的设计和实施中，涉及的技术主要有以下几种：

① 网络技术　包括局域网(LAN)和广域网(WAN)的常规技术，应确保所设计的网络无网络瓶颈，并能够向网络中的用户提供足以进行内网(局域网)交流和外网(Internet)访问所需要的带宽。

② Internet/Intranet 技术　应当包括 TCP/IP 协议和 WWW 技术及其所提供的各类服务。

③ 信息制作与发布技术　包括信息的划分、信息资源页面的设计、发布与链接。

④ 安全技术　应当包括网络操作系统提供的安全管理技术、数据保护技术、防黑客攻击技术、计算机和网络防病毒技术等。

7. 规划设计的具体内容

① 物理网络的主干网的设计与设备选型。

② 网络操作系统的选择，以及所选网络操作系统与所确定的网络服务子系统的集成技术的确定。

③ 根据所在单位信息系统的具体要求，选择和确定中间件、数据库平台，以及所要开发的应用系统。

④ 根据信息应用系统的设计目标，选择开发主页的制作工具、信息发布和开发的工具。

⑤ 确定 Internet 的接入技术。

⑥ 确定代理服务系统。

⑦ 安全技术。应根据用户对其数据的保密性要求，确定需要的安全等级，以及所采用的技术和投资费用。

⑧ 如果需要建立可供外部用户随时访问的站点，则需要申请域名或静态 IP 地址，并根据内部网络的分布情况划分子网 IP。

⑨ 网络经费预算。应当分为一次性投资和维持运行两部分。包括硬件、软件、安装与调试、培训与服务费用，以及网络的安全、维持和运行费用等。

⑩ 完成上述工作之后，应根据实际情况确定详细的工程设计、建设、进度和施工的计划。

5.1.2　Intranet 的规划设计与架设

本小节介绍在进行小型 Intranet 设计与实施过程中应考虑的一些问题。

1. Intranet 规划设计的主要步骤

Intranet 的设计一般应在网络规划的基础上依次进行，对于中小型 Intranet 的规划与设计步骤归纳起来有如下几项：

(1) 用户需求分析和网络需求目标的确立

① 分析用户所在单位的状况　包括设备与人员的现状、预计投资状况、网络中站点分布情况、数据的流量与流向以及当前通信线路的情况。

② 确定网络的功能和性能目标　根据用户的需求，确定网络建成后可以实现的近期和远期目标，以及相应的网络功能。

③ 成本和协议的核算　对所要建设的网络的成本和可能带来的经济效益和社会效益进行分析，并由此产生该工程项目的可行性报告。

④ 编写需求分析报告。

(2) 网络系统方案设计

在用户需求分析的基础上进行的网络系统方案的设计是 Intranet 系统集成的核心。网络系统方案设计包括下述几个主要部分：

① 设计 Intranet 的内部物理网络　根据前面所介绍的步骤和方法，在网络需求分析

和规划的基础上，针对各种不同的规划方案，对其网络性能、投资和维护费用进行综合的分析和比较，最终确定网络系统的规模、拓扑结构、主要部件，并制定出具体的配置清单、工程的实施计划和设计说明，为 Intranet 内部物理网络的建立做好技术准备。在进行物理网络设计时应当包括的内容如下：

- 确定网络的规模　指确定网络覆盖的范围和边界。
- 确定网络的应用范围　指确定网络的应用领域。
- 确定网络的模式　指确定网络的总体模式，例如，是采用 C/S(客户机/服务器)模式还是采用 B/S(浏览器/服务器)模式，网络的管理是集中式还是分布式。
- 确定网络拓扑结构　指根据信息点的分布与信息的流向，选择合适的网络拓扑结构，并确定网络节点设备的功能和大小。

② 设计和确定 Internet 的接入技术和方式　在 Intranet 内部物理网络的设计基础上，首先，应当选择邮政部门所能提供的服务；其次，确定接入 Internet 的方式和设备，并对这两部分做出多种方案的投资、维持、运行和管理等费用的比较。

③ 选择和确定网络安全的措施　网络安全的措施可以从硬件可靠性、备份策略、访问控制技术、防病毒技术、容错技术以及防火墙技术等多方面进行选择和设计，以确保网络的安全性和可靠性。

④ 结构化工程布线的设计　指在网络中，对全部的传输介质实施结构化的布线设计和施工设计。

(3) 计算机系统和应用系统的选择和设计

计算机系统的选择和设计中最主要的是选择和设计好软件平台。设计人员应当根据企事业单位的环境和信息系统的具体要求选择软件平台。

① 网络操作系统的选择　包括服务器和客户机软件平台的确定。例如，根据前面叙述的准则和用户的功能需求，选择了如下的服务器和客户机的软件平台。

- 服务器端软件　选择了 Windows NT Server 4.0 或 Windows 2000 Server 版，它们均集成了多种应用服务器及其管理功能，如文件服务、WWW、FTP、RAS(远程访问服务)、DNS(域名服务器)等。
- 工作站端软件　Windows 95/98/NT/2000 等作为网络工作站的软件平台，这些软件中都具有很好的内置网络功能和浏览器。

② 确定信息系统的开发平台　即根据用户需求和应用需要选择数据库管理系统、开发工具及其他必要的功能性软件。例如，选择可以与上述网络操作系统很好地配合的微软公司的 SQL Server 和 Exchange Server(邮件服务器)等。

③ 确定必要的管理软件　根据网络的规模确定网络管理的工具和软件。

(4) 选定硬件设备和机房环境

根据上述步骤所确定的网络系统设计方案，选择性能价格比较高的硬件设备。对较大规模的网络，机房设计也是不可缺少的，其中包括服务器机房环境、工作站机房环境、打印机房与其他共享设备(如高、中档绘图仪和扫描仪)环境等多种环境的温度、湿度和通风等参数的要求。

(5) 编写网络系统集成的详细技术文档

网络系统集成的详细文档是以上各个部分规划与设计的集成，并由此生成网络系统的最终技术文档。

(6) 物理网络的安装和调试

安装和调试物理网络，例如，安装和调试局域网中的各种设备、网络互联设备，铺设和测试传输介质等。

(7) 网络功能子系统的安装和调试

安装和调试网络中选定的各个服务子系统，例如，实现 WWW 和邮件服务等。

2. 小型 Intranet 物理网络结构的设计与架设

(1) Intranet 内部局域网的网络结构设计

① 拓扑结构　常见的拓扑结构有总线型、星型、环型、树型和网状等多种类型。每种类型都存在着不同程度上的优点和缺点。在实际的网络设计中，通常不是单一的网络拓扑结构，而是根据需要进行了综合设计的结果。在实际设计中，往往是先确定主干网，再对子网进行适当的组合设计。在中小型局域网中，常见的物理拓扑结构为“星型”或“树型”，其中“树型”可以看成是“星型”拓扑的扩展。这两种结构都有较好的可管理性、性能价格比、可扩充性和兼容性。

② 传输介质　中小型局域网通常选择 3 类、5 类或超 5 类的非屏蔽双绞线(UTP)。考虑适应未来的发展，新建网络应选择 5 类或 5 类以上的非屏蔽双绞线，即支持 100Mb/s 及以上的数据传输速率。

③ 中小型局域网的网络系统结构实例　假定选择如图 5-1 所示的 100/10 Base-T 交换式以太网作为中小型企业内部网络。

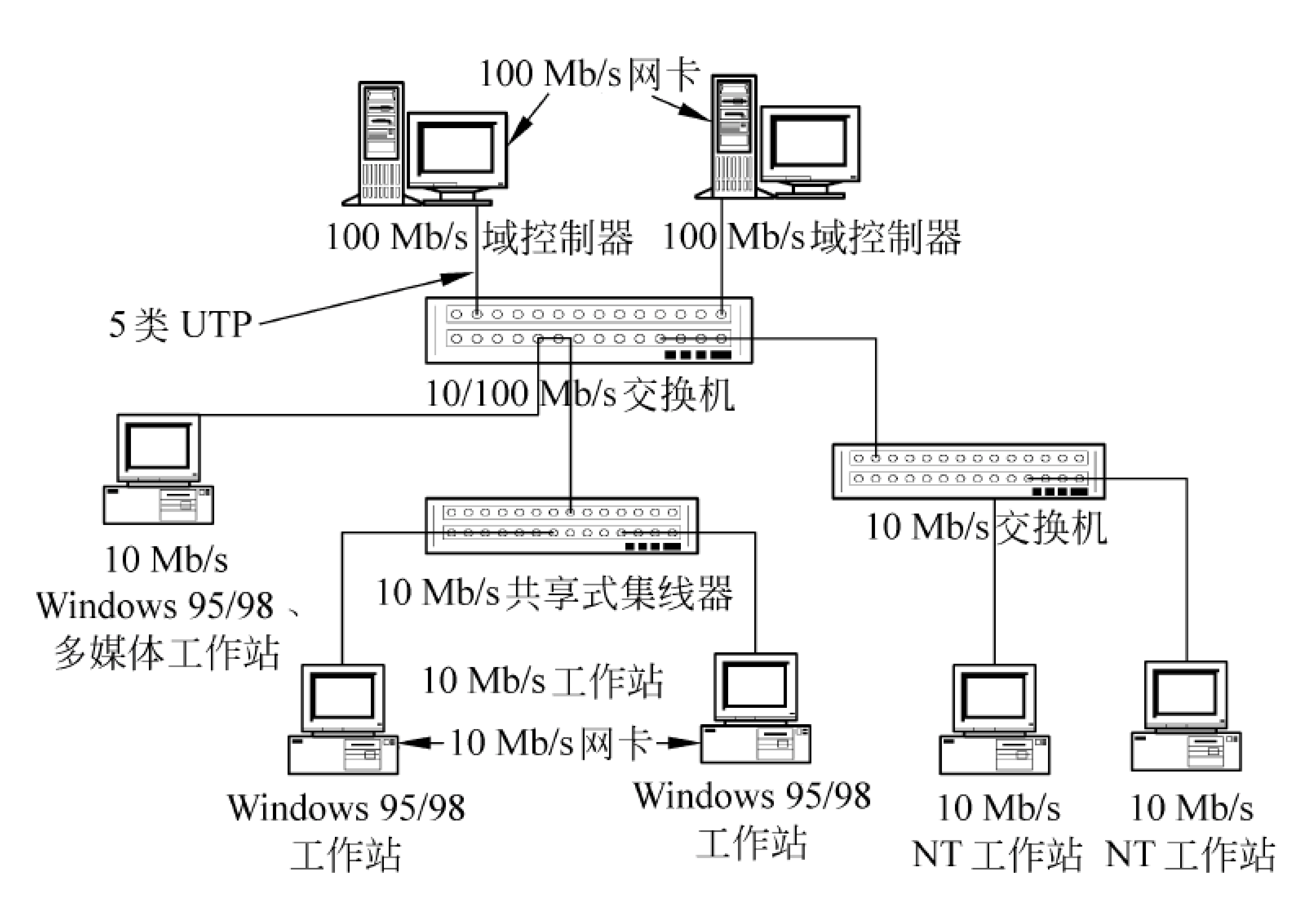


图 5-1　100/10 Base-T 交换式以太网

(2) Intranet 内部局域网的组成部件设计

Intranet 的硬件结构与局域网的结构没有太多的区别，一般可以按局域网的方法构建。Intranet 的实际结构如图 5-2 所示。

由图可知，实用 Intranet 的实体应包含以下几个部分：

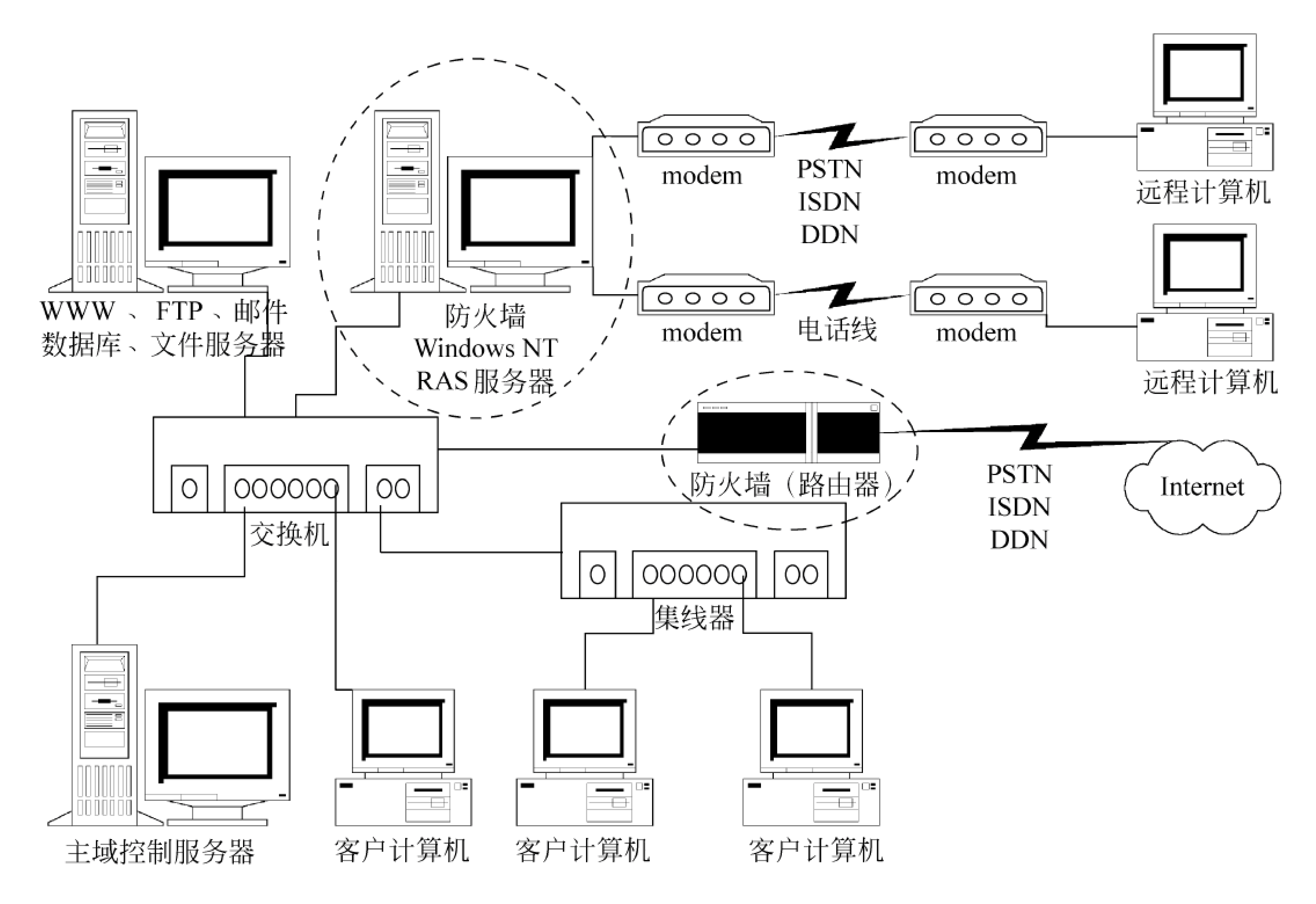


图 5-2　中、小型企事业单位 Intranet 的实际结构

① 服务器　服务器主机是整个 Intranet 的核心部件，它们为整个网络提供网络管理、网络服务和信息服务。服务器的主机根据它所提供的服务分为两大类，即网络服务器和应用服务器。

- 网络服务器就是提供网络控制、管理和常规网络服务的主服务器。在大型网络中分为主干网服务器、部门网服务器和工作组网服务器。在中小型网络中，常常就是指安装了网络操作系统的服务器。例如，Windows NT 网络中的主域控制器(PDC)和远程访问服务器(RAS)；Novell 网络中安装了 NetWare 软件的文件服务器等。它们在网络中提供各种网络管理、网络服务和远程访问服务。
- 应用服务器就是提供各种应用的服务器，常见的应用服务器有：提供信息服务的服务器、WWW 服务器、FTP 文件服务器、通信(电子邮件)服务器、打印服务器、数据库应用服务器等，这些服务器可以为网络用户提供信息资源的传递、访问和信息共享等信息服务。根据需要可设置一个或多个服务器的硬件实体。例如，使用一个实体可以同时实现 Web 服务器、数据库服务器、邮件服务器和打印服务器等多种功能。

由于在网络为中心的计算机环境下，服务器是最主要的设备。因此，各种服务器通常要求具有较高的性能，例如，具有可靠性高，吞吐能力强、内存容量大、连网功能强等性能，但是不同的服务器对硬件的配置要求各不相同。一般网络的主干服务器对 CPU、内存容量、硬盘容量和可靠性等要求较高；而 WWW、FTP、数据库服务器和邮件服务器需要较大的硬盘空间，以便存放信息和数据资源；数据库服务器还需要高速的 CPU 和较大容量的内存。

② 工作站(客户机)　目前,Intranet 常采用 C/S 或者 B/S 模式,由于网络工作站是网络客户的硬件平台,因此,也被称作客户机,其硬件的配置应当根据其工作类型而确定。客户机也是网络用户使用共享资源的接口,用户通过它提出服务请求,并返回服务器处理的结果信息。目前,客户机通常是普通 PC 机,用户通过上面安装的浏览器软件,即可浏览服务器和网络上的各种信息。

设计时,应根据需要确定工作站的类型,以及支持 Intranet 资源访问系统需要的软件。例如,选择 Pentium Ⅲ 微机作为一般办公室的客户机,同时可以选择 Windows 95/98/ NT Workstation /2000 或 DOS 等作为工作站的桌面系统的软件平台。

③ 物理网中的通信子网　除了上述网络中的主机外,物理网还包括 Intranet 的通信子网,它是通信的基础设施。一般包含以下几个基本部分:

- 传输介质与传输介质的连接器,例如 5 类 UTP、RJ-45 连接头和网卡;
- 网络共享的连线和互联设备,例如中继器、集线器、交换机、中继器和路由器等。

④ 防火墙(firewall)　防火墙是网络安全的屏障,通常由硬件和软件系统组合而成。防火墙通常设置在"被保护网络"(局域网的内部网络)与外网(如 Internet)之间,如图 5-2 中虚线所示。一个防火墙可以是一台路由器、一台主机,或者是一个主机群。

⑤ 网络中需要的其他共享设备　除了上述设备之外,网络可能还需要用户提出的其他共享设备,例如网络上的打印设备、扫描仪和高级绘图仪等。

(3) 小型企业网络的设计和实施实例

① 确定网络的结构和部件。

选定网络结构为 100/10 Base-T 交换式以太网,如图 5-1 所示,并根据各种网络服务子系统的需要确定了如下的部件:

- 网络主要服务器的确定和选择　包括网络服务器和网络应用服务器,例如,设置了一台 PDC(主域控制器,兼作信息服务器和 Web 服务器)、一台 BDC(备份域控制器兼作打印服务器)和一台数据库服务器(兼作邮件服务器)。
- 网络主干连接设备和传输介质的确定　选择一台速率为 10/100Mb/s 的 8 口或 16 口交换机,含有满足需要数量的 100Mb/s 口,若干 5 类 UTP 和 RJ-45 接头,多台共享式及交换式集线器。
- 网络瓶颈问题的解决　将系统的 PDC 和 BDC 接入交换机的 100Mb/s 专用端口,将 10Mb/s 的交换式集线器和共享式集线器接入交换机的 10Mb/s 共享端口,将需要专有带宽的工作站接入交换机的 10Mb/s 专有带宽端口(如多媒体工作站)。
- 网卡　目前市场上最常见的低端网卡是 NE2000(16 位 ISA)和 Realtek(32 位 PCI)及其兼容系列的产品,高端产品通常是 3Com 或 D-link 公司的产品。设计时,应当按设计的规格更换或购买需要数量的网卡。例如,本例需要两个速率为 100Mb/s 的、含有 RJ-45 接口的 PCI 网卡;若干速率为 10Mb/s 的、含有 RJ-45 接口的 PCI 网卡。
- 布线工程　根据需要铺设或更换传输介质。例如,布线、连接线的制作、安装信息模块和插座、连通线路、测试线路;接线柜的布置、安装和接线的标记;施工图、接线架、各种网络设备、接线柜等的连接图绘制。

- 设计中还应当考虑最远点工作站与网络的连接，即解决传输距离的问题。

② 10/100Base-T 交换式网络的架设。

架设时，所需要的器材和施工步骤如下：

- 准备好若干 RJ-45 水晶头（接头）和非屏蔽双绞线。根据干线和支线的不同要求分别配置 3 类、5 类或超 5 类 UTP。
- 根据需要，使用专用工具和测试仪器制作好连接用的网线。例如，制作符合 TIA/EIA 568B 和 568A 标准的标准线和交叉线，应注意 10/100Base-T 网络电缆长度最长为 100 米。
- 将交换机、交换式集线器或集线器等网络共享设备安装和连接到位。
- 每一个网络节点设备，通过自身的网卡、非屏蔽双绞线和交换式 Hub（或交换机）连接成物理上的星型或树型拓扑结构，如图 5-2 所示。
- 按照单、双、或多个集线器的 10/100Base-T 双绞线以太网的组建、施工、配线要求的方式进行网络的架设、连接、施工和检测。

上述步骤完成之后，可以进行 Windows NT Server 及有关网络软件系统的安装、调试过程。

③ 网络安全系统的设计与实施。

网络安全系统的设计与实施过程，参见本书的第 12 章远程管理和第 15 章网络安全管理等章节的内容。

(4) 中小型 Intranet 内网与外网连接方式的设计实例

在第 2 章已对不同的接入技术做过介绍，本节将介绍几个适合中型以上企事业单位使用的 Intranet 实例，即 LAN 通过公用广域网与 Internet 互联的应用案例。

① 局域网互联或接入 Internet 的方案。

公用电话网是全球最大的通信网络，其实质是一个世界范围的广域网。因此，通过公用电话网，可以很容易地实现局域网通过公用广域网与 Internet 之间的互联。使用公用电话网互联网络时，最常使用的是远程访问服务器和调制解调器。

- 通过拨号电话线接入 Internet 的方案　中型以上企业通过拨号电话线接入 Internet 的方案如图 2-6 所示，这是使用电话网实现互联的典型案例。使用此方案时，需要先通过公用的拨号电话线建立起拨号连接，再进行数据传输，因此，适用于数据传输量不大、无需持续传输和传输速率要求不高的场合。
- 通过租用电话专线接入 Internet 的方案　中、大型企业通过租用电话专线接入 Internet 的方案如图 2-7 所示，其最大特点是：任何时候均可以使用，无需拨号建立连接，因此，适用于大量的、持续性数据通信和高速数据传输需要的场合。

② 局域网使用公用电话网的互联实例。

ⓐ 用户需求如下所述：

- 满足 100 人左右的用户流畅地访问 Internet；
- 实现 Internet 上的特权用户访问局域网内部服务器；
- 公司内部对外提供 WWW、FTP 和 Telnet 服务；

ⓑ 规划设计特点：

- 使用包过滤“路由器”,禁止局域网内的特定主机访问 Internet;
- 使用包过滤“路由器”,可以防止外部非法用户对内部网络的访问,也可以允许 Internet 上的特权用户对内部网络的合法访问;
- Internet 主线路发生故障后,能自动启用备份线路;
- 公司规模进一步扩大后,路由器要有较好的扩展性及适应性。

ⓒ 具体设计方案。方案如图 5-3 所示,利用一台路由器实现企业内部网接入 Internet 和网络安全控制;利用联想 BDCOM3081 路由器的广域网口:WAN1 或 WAN2 端口与同步基带 modem 相连,然后通过 DDN、frame-relay 或 X.25 等专线与 ISP 连接构成主链路,可以充分保证用户连接的带宽和数据传输的可靠性。

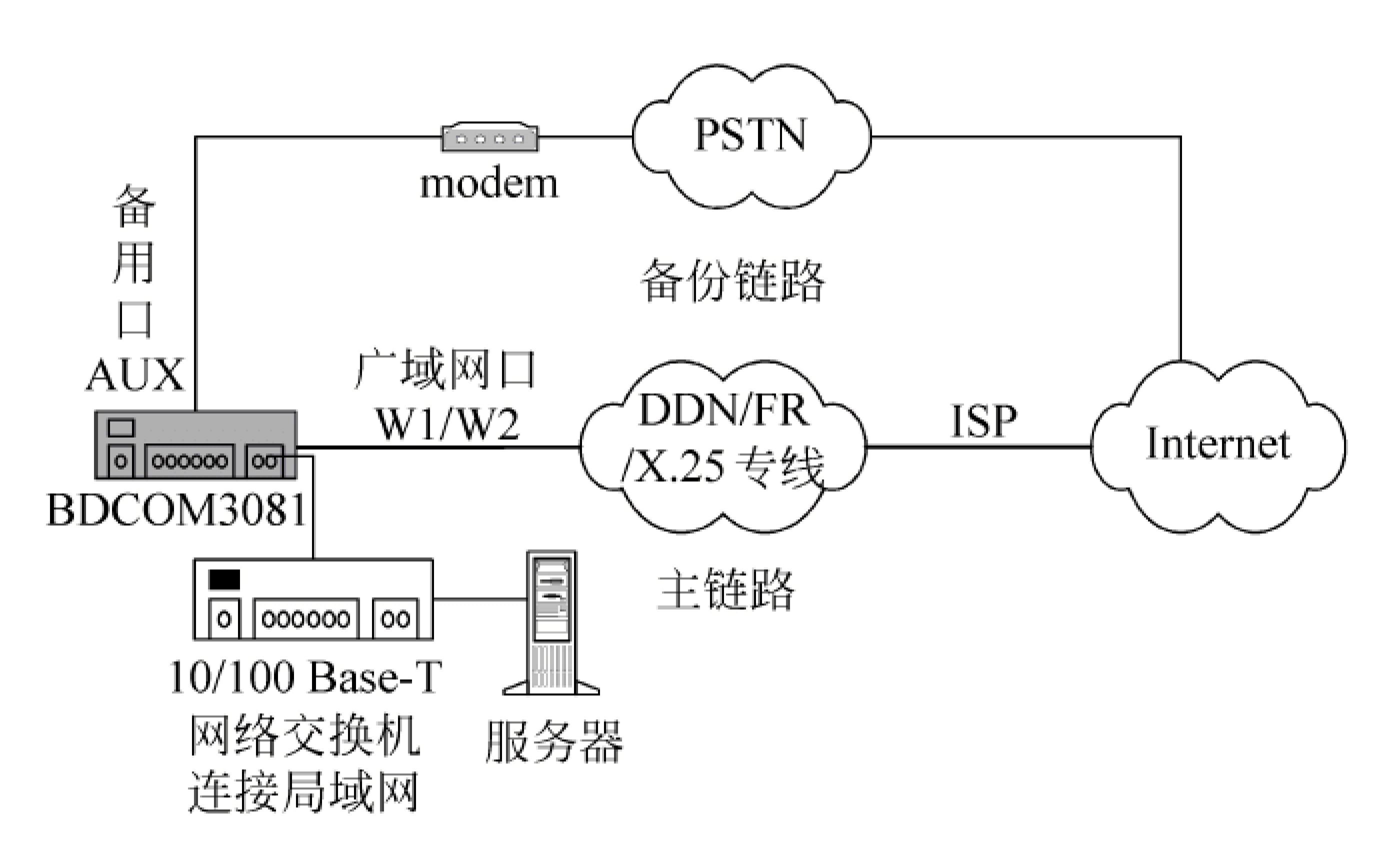


图 5-3 用路由器实现局域网对 Internet 的连接

ⓓ 方案的主要特色:

- 上网的速度高 DCOM3081 的 WAN1(W1)端口支持 V.24 和 V.35 标准,本方案使用 V.35 标准的基带 modem 与 WAN1 端口相连,最大带宽可达到 2.048Mb/s (E1)。
- 有效的安全措施 由于 BDCOM3081 路由器提供防火墙功能,支持基于 IP 地址、端口、协议、服务等的包过滤和访问控制策略,因此可以为企业内部网提供全面有效的防护,增强内部网络的安全性。通过路由器提供的 filter 和 access 等命令,可以根据需要设置一定的访问控制策略,防止外部非法用户对内部网络的入侵,也可防止内部合法用户对外部不安全站点或非预期站点的访问,同时还可以允许 Internet 上的特权用户对内部网络的合法访问。
- 有效的自动故障处理和保证体系 本方案中,使用 BDCOM3081 路由器的 AUX 备份口连接模拟 modem,然后经 PSTN 线路接入 Internet 形成备份链路。当主链路发生故障时,路由器自动启用 PSTN 备份线路,通过普通 modem 异步拨号访问 Internet。当主链路恢复正常后,路由器自动切断备份线路并启用主链路。
- 有效的电源支持保证措施 BDCOM3081 提供双电源备份,用户可接两条独立的电源线,当某一条线路出现故障时,仍能保证电源供应的连续性。
- 良好的扩展性能 由于联想 BDCOM3081 提供多种端口,并提供扩展插槽,支持众多的功能模块,从而可以实现多网络互联和多用户访问 Internet 方案,因此上

述方案为企业内部网络以后的扩展留有较大的余地，可以最大限度地保护用户的投资。

5.1.3 Intranet 中网络操作系统的确定

网络操作系统的英文为 network operation system，其缩写为 NOS。网络操作系统的选择是网络设计中非常重要的一个环节。由于 NOS 对于网络的整体性能起着决定性的作用，因此，选择合适的网络操作系统可以大幅度提高系统的效率，达到节约金钱和物力的目的。

1. 网络操作系统的分类

目前流行的网络操作系统主要有：UNIX、NetWare、Microsoft NT/2000 和近年来流行的 Linux。进入 20 世纪 90 年代以来，计算机网络互联、不同网络的互联等问题已成为热点。所以，网络操作系统便朝着能支持多种通信协议、多种网络传输协议、多种网络适配器和工作站的方向发展。下面将简单介绍几种常见的网络操作系统。

（1）UNIX 网络操作系统

UNIX 操作系统常用的版本有 AT&T 和 SCO 公司推出的 UNIX SVR3.2、UNIX SVR 4.0，以及由 Univell 推出的 UNIX SVR4.2 等。目前 UNIX 的应用重点是在大型网络的高端网络。在 Internet 中较大的服务器上都无一例外地使用了 UNIX 操作系统，众多的 Internet 的 ISP 站点也都还在使用 UNIX 操作系统。由于 UNIX 系统不易被普通用户掌握，因此，在一般的中小型网络上很少使用 UNIX。

（2）NetWare 网络操作系统

NetWare 以其先进的目录服务环境，集成和方便的管理手段，简单的安装过程等特点，受到用户的好评。由于它对微机的硬件环境要求不高，对无盘工作站支持较好，因此，NetWare 适合应用在利用原有计算机组网，计算机档次不高，或配置较低的中小型局域网。例如中学教育网、实验室和游戏厅等场所。

（3）Windows NT/2000 网络操作系统

Windows NT/2000 提供了多种功能强大的网络服务功能，例如文件服务器、打印服务器、远程访问服务器，及 Internet 信息服务器等。Windows NT 4.0 和 Windows 2000 Server 的操作不仅具有 Windows 95/98 的统一界面和方便性，而且其系统结构是建立在最新操作系统的理论基础上的。因此，在系统的稳定性和安全性要求不是很高的中小型网络中，人们常常使用比较容易掌握的、有一定安全保护功能的、稳定性较好的 Windows NT/2000 作为网络操作系统。本书就是以 Windows NT 为主线来管理中小型 Intranet 的，因此，有关它的许多功能、特点及使用，将在后续的章节中逐一作介绍。

（4）Linux 网络操作系统

Linux 是建立在 UNIX 基础之上的一个版本。最初是由 Linus Benedict Torvalds 等通过 Internet 组织起来的开发小组编写的，后来又有众多软件高手参与开发，并使之不断完善，它功能强大，具有丰富的系统软件和应用软件的支持。另外，它还是一个开放使用的自由软件。

由于 Linux 具有可以与其他操作系统相媲美的多任务、多用户、多平台、多线程、虚拟

存储管理、虚拟控制台、高效磁盘缓冲和动态链接库等强大的应用功能，因此，可以说Linux是一种可以与Windows抗衡的、极具发展潜力的操作系统。Linux适用于需要运行各种网络应用程序，并提供各种网络服务的场合。正是由于Linux的源代码开放，才使得它可以根据自身的需要做专门的开发，因此，它更加适合于广大需要自行开发应用程序的用户和那些需要学习UNIX命令的用户。

综上所述，NetWare、Windows NT/2000和Linux均可用于微机，其中：NetWare和Linux对硬件的要求不高，而Windows NT在低配置机器上的性能不如前两者稳定，Windows 2000对系统的硬件配置要求较高。UNIX通常只兼容某些型号的工作站的专用机型，因此，一般用于金融、电信系统等部门的核心网络中。

2. 网络操作系统的选择

由于常见的网络操作系统各具特色，而且涉及到一系列的技术问题，例如，它涉及到网络的拓扑结构、网络服务器支持、网络的站点访问、网络连接设备的支持、网络内部连接方式、工作站内存的占用、网络的容错功能、网络的管理和安全性等多方面的因素，所以选择网络操作系统时应当考虑如下几个方面：

① 符合国际标准和工业标准　选择网络操作系统时，应当先从其性能和标准化两方面进行考虑。

② 兼容性　选择网络操作系统时，硬件的兼容性也是需要重点考虑的因素。这里兼容性主要指能支持多种网络硬件设备。

③ 网络规模　各种NOS对网络客户的数量均有限制，因此，应当根据用户网络的规模进行选择，在考虑网络规模时，注意留有充分的扩充余地。此外选择时，还要注意所选NOS在既定数量用户运行时，系统的稳定性如何。

④ 可靠性　在所介绍的4种网络操作系统中，比较起来，Windows NT/2000的功能较强，可靠性相对较低，如果企业的保密性要求不高，功能要求较强，则应当选择NT。否则，应当选择安全性能较好的NetWare、UNIX和Linux。

⑤ 对远程通信的支持　各种NOS都提供了许多远程通信的工具。例如，新版本的NetWare和Linux本身就集成了路由器和网关的功能；而Windows NT在远程通信时，需要对外部来的IP包进行转换，因而降低了效率。

⑥ 能获得众多的应用软件并支持现有的应用　凡是有众多应用软件支持的网络操作系统一般也是市场占有率较高的操作系统。

⑦ 应具有良好的管理功能、方便的开发平台以及安全保证　NetWare 4.X和Windows NT 4.X以上的版本都具有良好的菜单系统和强大的管理功能。具有友好、方便的开发平台的操作系统可以使用户高效地开发自身的网络应用程序；而良好的网络安全功能则是确保用户使用的重要前提。在选择网络操作系统时，应当考虑它提供给用户的访问权限。例如，NetWare 4.X和Windows NT/2000操作系统都可以给用户提供4级安全保证、授权、目录和文件保证等功能。

综上所述，对于高级应用的场合，或者安全性能和稳定性要求较高的大型网络，应当选择UNIX；而对于中小型企业来说，由于Windows NT/2000具有简单易用、界面友好、管理方便和功能日益强大等特点，并且它可以运行几乎所有的新版大众化软件，并且支持

多处理器操作，可扩展性也很好，还能够为用户的应用程序提供更多的内存，因此，日益受到中小型企业用户的青睐。目前，人们广泛使用 Windows NT 4.0，或者是 Windows 2000 来组建办公网、工商企业网和校园网等中、小型的 Intranet，它们也因此而成为当前较流行的网络操作系统。

在本书的后面章节中将介绍如何使用 Windows NT 网络操作系统建立、管理一个实际的局域网和 Intranet。

5.1.4 Intranet 中网络服务子系统的确定

Intranet 除了具有局域网的基本功能外，更重要的是能够为网络用户提供信息服务。常见的 Intranet 中基本的网络服务子系统有：网络服务器服务、DNS 域名服务、WWW 服务、FTP 服务、邮件服务、DHCP 服务和打印服务等几种基本类型的服务。为了提供上述这些服务，Intranet 中需要安装、设置和管理相应的服务子系统软件，而所需要设置的服务器的类型和数量应当根据用户的需求而定。例如，一般可能会有网络主服务器、WWW 服务器、FTP 服务器、数据库服务器、打印服务器，以及邮件服务器。当然，如果网络的规模较小，这些服务器的软件可以安装到一台服务器的实体上。例如，在较小的 NT/2000 网络中，可以把这些软件安装和集成在主域控制器中；反之，如果网络的规模较大，则可以分别安装到多台服务器上。下面将介绍一下这几种网络服务子系统的功能和软件的选择。

1. Intranet 中网络服务子系统的设计

(1) 网络服务器服务子系统

① 网络服务器服务子系统的功能。

网络服务器服务子系统的主要目的是实现 Intranet 内部用户的组织和管理，并提供网络上硬件、软件和数据资源的共享、服务和管理。

此外，为了在 Intranet 上使用 Internet 技术，实现统一方便的信息资源的共享，还要在 Intranet 的主控服务器中选择和配置 TCP/IP 协议，只有这样，才能实现 Intranet 服务器的各项子功能。

② 网络服务器服务子系统使用的软件。

- 服务器端软件　网络服务器服务子系统中最重要的软件就是网络操作系统。该软件通常安装在主控服务器上，并在网络环境下实现基本管理，并能提供网络资源服务。例如，在使用 Windows NT/2000 组建的 Intranet 中，通常需要至少一个安装了 Windows NT/2000 Server 的“主域控制器”，它可以对用户进行网络用户、文件与目录管理等，并提供必要的网络服务；还可以管理客户机上的账户、共享资源和设备等。
- 客户工作站端软件　当组建一个 Intranet 时，在选择了网络服务器端软件之后，通常还会选择与其配套的客户机软件。例如，在使用 Windows NT Server 组建的 Intranet 中，其客户工作站的软件通常为 Windows NT Workstation 或 Windows 98/2000 专业版等。

(2) DNS 域名服务子系统

DNS 担负着将形象的域名翻译为计算机可以接受的数字型 IP 地址的工作。有了 DNS 服务器，就可以在 Intranet 内使用域名访问各种资源。DNS 子系统使用的软件如下：

- 服务器端软件　例如，使用 Windows NT/2000 Server 中集成的 DNS 服务，即可建立起 DNS 服务器。
- 客户端软件　例如，在各客户机上，利用和配置 Windows 95/98/NT/2000 上 TCP/IP 协议中的 DNS 卡，即可启用 DNS 客户机功能。

(3) WWW 服务子系统

在 Internet 和 Intranet 中，WWW 服务子系统不仅提供图形界面的快速检索与查询功能，还通过各种各样的"中间件"（接口）和 Web 服务器进行连接，从而可以实现容易掌握的、基于浏览器的瘦客户技术类型的信息交流与共享的手段。为此，WWW 服务子系统也成为 Intranet 中最重要的组成部分，可以说没有它就不是真正的 Intranet。有了 WWW 子系统才可以在 Intranet 内以 WWW 方式使用各种信息资源。WWW 子系统使用的软件如下：

- 服务器端软件　常见的适于组建 Intranet 的 Web 服务器软件有微软的 IIS（Internet information server，为部门级的 Intranet Web 服务器软件）、Netscape Enterprise Server（企业级的 Intranet Web 服务器软件）、Novell NetWare WebServer 和 Oracle WebServer 等。例如，IIS 运行在 Windows NT/2000 服务器上，可以建立 WWW 服务器和 FTP 服务器，具有较好的安全性能，支持各种数据库软件，与 SQL Server 一起使用可以提供数据库的最佳连接，此外，还提供了 CGI、ISAPI 和 ASP 等各种编程接口，可以制作动态网页。
- 客户端软件　主要包括 WWW 浏览器软件（HTML Browser）、主页制作软件（HTML Editor）和主页转换软件（HTML Converter）等，这些软件的功能都可以通过使用 IE 和 Netscape 中的相应功能而实现。

(4) FTP 服务子系统

FTP 是 TCP/IP 协议族中的有关文件传输的协议。使用 FTP 协议可以通过网络从一台计算机向另一台计算机上传送文件。FTP 子系统的主要功能是在 Intranet 上实现与 Internet 方式类似的网络上的文件传输，向用户提供各种类型的软件、应用程序和文件资源。FTP 子系统使用的软件如下：

- 服务器端软件　如使用 Windows NT Server 4.0 和 Windows 2000 Server 软件中的 IIS 建立 FTP 服务器。
- 客户端软件　使用 Windows 95/98/NT/2000 内置的 FTP 功能时，既可以直接运行 FTP 程序，也可以通过 IE 浏览器中的"ftp://"方式调用 FTP 功能。当然，还可以使用专用的 FTP 上传和下载软件，例如 Cute_FTP 和 WS_FTP 等。

(5) 电子邮件(E-mail)服务子系统

电子邮件是一种廉价、快捷、方便、高效的多种信息交换的工具，因此，电子邮件服务子系统是 Internet 和 Intranet 中最基本的子系统。其主要作用是提供通信服务，即让客户机通过网络上的电子邮件服务器，能够有效地交流信息。电子邮件子系统使用的软件

如下：

- 服务器端软件　可以使用 NT 中内置的工作组邮局或 MS SMTP Server，也可以使用 Exchange Server 和 Lotus Notes 等软件。
- 客户端软件　IE 集成的 Outlook Express、Fox Mail、Office 中集成的 Microsoft Outlook 和 Netscape 中的电子邮件功能等。

(6) 代理服务器(proxy server)服务子系统

① 代理服务器子系统的功能。

- 提供 Internet 连接共享，即代理局域网中的客户机，或者其他计算机连入 Internet 并使用其中的各种共享资源。
- 作为防火墙，既可以完成 Intranet 与 Internet 的互联，又可以防止外部用户非法访问企业内联网 Intranet。
- 作为 WWW 服务的本地缓冲区，将 Intranet 用户从 Internet 中访问过的主页或文件的副本存放在代理服务器中，用户下次访问该信息时，可以直接从代理服务器中取出，这样可以大大提高用户的访问速度，节省费用。

② 代理服务器子系统使用的软件。

- 服务器端软件　各种代理服务器的软件非常多，用户可以在各个网站上查询，例如，查询网站“华军软件园”和网址 http://www.newhua.com.cn。在 Windows 98/2000 上实现共享 Internet 的软件中最常用的代理服务器软件是 ICS、WinGate、SyGate，以及在 Windows 95/98 上运行的 Proxy Server 2.1/3.4.1 等。

注意：代理服务器的服务器端软件应当安装在已经安装了 IIS 的服务器上，这些服务器还应当与 Internet 直接或间接相连。

- 客户端软件　如果是实现浏览器的共享，可以使用 IE 或 Netscape 的内置功能；如果是实现 FTP、Telnet 和 E-mail，则还需要进行相关客户端软件中网关(gateway)的设置。

(7) 远程访问服务(RAS)子系统

远程访问服务的英文缩写为 RAS(remote access service)。所谓远程访问服务就是指在办公室以外的用户，可以使用电话线连入局域网并存取网络资源，从而使办公地点扩展到办公室以外的任何地方。RAS 系统使得远程客户的工作就像在本地网络中一样。

大型单位可以采用第 2 章中所述的设备实现远程访问，例如，使用专用远程访问服务器的网络系统结构，如图 2-6 所示。对于小型单位可以采用如图 5-1 所示的结构实现远程访问服务。远程访问服务系统使用的软件如下：

- RAS 服务器软件　可以使用专用远程访问设备配置的软件和网络操作系统内置的远程访问功能。例如，直接使用 Windows NT/2000 中的 RAS 服务功能。
- 客户端软件　可以使用 Windows 98/NT/2000 中内置的拨号网络服务和所需的通信协议来实现远程拨号连入 Intranet 的功能。

(8) 应用服务子系统

在 Intranet 中仅有上述子系统是不够的，企事业单位用户还需要开发和建设内部网

络的各种应用子系统。其中，数据库服务器就是 Intranet 上应用子系统的一个重要组成部分，目前用户常通过 Web 服务器访问、使用各种网络上的信息资源。而 Web 服务器一般是通过诸如 ODBC（open database connection）等接口与数据库接口相连接的，ODBC 目前已为大部分数据库厂商所接受，各种数据库都提供了 ODBC 接口，并且都可以通过 WWW 形式表现出来。主页制作人员在 WWW 主页中嵌入 SQL 语句，用户就可以直接通过主页访问数据库文件。

在上述子系统中使用的软件需要根据系统的类型而定，如，B/S 结构和 C/S 结构使用的软件就有所不同。为了适应 Internet 和 Intranet 中 WWW 直接与数据库连接的要求，很多公司推出了“数据库-WWW”数据转换工具、开发工具、中间件和报表生成工具等，用户应根据自己的实际情况进行选择。

2. Intranet 中网络服务子系统的实施过程

Intranet 的构建与其他项目一样，在建设之前，都应当进行很好的规划和设计。通常包括需求分析、目标论证、经济论证（即投资和维持费用权衡比较）等几个主要部分。Intranet 的构建具有很大的弹性，不同规模的单位所建立的 Intranet 的规模的大小、层次、功能可能会相差很大。对于已建好局域网的单位，可以充分利用现有资源，在现行网络的基础上改造、扩充。前面已经介绍了 Intranet 硬件的实施方法和过程，本节将介绍各个网络服务子系统软件的安装和调试步骤。

对于系统软件和应用软件的安装和调试，一般应当按照服务器端和客户端两大部分进行配置和管理。

(1) 服务器端的配置和管理

① 安装网络服务器的操作系统。例如，安装和设置 Windows NT Server 4.0 或 Windows 2000 Server。

② 建立域名服务器。例如，安装和设置 Windows NT/2000 Server 中的 DNS 服务器，配置虚拟主机。

③ 建立 WWW 服务器。例如，安装和设置 Windows NT/2000 Server 中的 IIS，建立 WWW 服务器和 FTP 服务器，设置好虚拟 Web 站点和目录。

④ 建立邮件服务器。例如，使用 Windows NT Server 4.0 中的工作组邮局建立邮件服务器，也可以使用 E-mail Server 第三方软件建立规范的电子邮局。

⑤ 设置远程访问（RAS）服务器和 Internet 的接入方式。例如，安装和配置 Windows NT Server 4.0 中的 RAS 服务器，并实现调制解调器（普通电话线）、ISDN NT1（ISDN 专线）、ISDN 路由器（ISDN 专线）或 DDN 路由器（DDN 专线）等各种接入方式下对 Internet 的访问。例如，通过 Windows NT Server 4.0 中的 RAS 服务器，可以完成对远程工作站的拨号访问控制功能，而通过路由器可以实现 LAN 用户对 Internet 的访问。

⑥ 建立代理服务器（Proxy Server）。例如，使用微软的 Microsoft Windows 98 SE/2000 中的 ICS、专用的代理服务器软件 WinGate 或 SyGate 都可以代理局域网内的 Windows 9X/NT 等平台上的用户，共享接入 Internet，还可以实现防火墙的功能。

⑦ 网络管理软件的安装与设置。网管软件可以实现对网络的自动监控和管理。

⑧ 完善网络安全的措施，实现防火墙功能。例如，实现预先设计的安全级别 C2 等

级,设置包过滤路由器,实现防火墙功能。

⑨ 开发基于 Intranet 的网络应用程序。例如,在 B/S 网络结构中,通过数据库服务器、数据库系统的开发工具、WWW 服务器和 Web 接口,建立起单位本身的网络综合信息系统,并实现与 Internet 一致的资源访问和浏览方式。

(2) 客户机(工作站)端的配置和管理

① 安装工作站网络操作系统。例如,安装和配置好 Windows 95/98/NT 工作站,或者是 Windows 2000 专业版的网络工作站,使得各个工作站可以正常连接网络服务器。

② 配置工作站上的 DNS,为企业网的域名服务做好技术准备。例如,配置 TCP/IP 协议中的 DNS 部分。

③ 启用网络工作站上的 WWW 浏览器,用以访问 WWW 服务器和网络上的各种信息资源。

④ 配置好网络工作站上的电子邮件功能。例如,使用 Windows 95/NT 或者 2000 工作站上的“收件箱”和 Windows 98 中安装的微软的 Office 中的组件 Outlook,作为客户机上的电子邮件软件,就可以收发电子邮件。

⑤ 配置好网络的远程工作站。例如,安装和设置 RAS 远程工作站,以实现远程工作站对网络的访问。

⑥ 设置好各网络工作站上“网关”中的 IP 地址。例如,该地址可以是代理服务器或者是路由器的 IP 地址,使得局域网内部用户可以访问 Internet。

5.2 使用 Windows NT 管理 Intranet

现代化网络管理集通信技术、网络技术和信息技术于一体,通过调度和协调资源,进行配置管理、故障管理、性能管理、安全维护和计费等管理,达到网络可靠、安全和高效运行的目的。Windows NT 网络管理主要指如何利用 NT 网络操作系统对一个 Intranet 进行管理。

5.2.1 Windows NT 网络管理的主要目标

对于管理一个实际的 Windows NT 网络来说,其主要目标包括以下几个方面:

① 建立和配置网络,提供网络服务,并向用户提供新的网络服务类型、增加网络设备和提高网络性能等。

② 组织和管理网络客户和共享资源。

③ 提供网络维护。主要包括网络性能监控、故障报警、故障诊断、故障隔离和故障恢复等。

④ 为提高网络利用率所采用的各种控制,即网络处理,主要指网络线路和设备利用率的采集、分析等。

⑤ 为实现预定的网络系统安全等级,在网络操作系统中采用各种安全控制技术。例如,实现 NT Server 中的身份识别系统控制、资源访问权限控制和安全审核,以及网络操

作系统的安全控制功能。

5.2.2 Windows NT 网络管理的具体内容

对于 Windows NT 网络来说，其管理通常包括以下几部分具体内容。对于其他网络操作系统而言，其常规的管理内容与 NT 网络类似，读者可以举一反三，参照本书的内容分别进行。

① 网络的基本配置管理　包括 NT 网络服务器、基本功能服务器（如 WWW、FTP、RAS 打印服务器和邮件服务器）和客户工作站的安装、配置，以及相应的系统配置与维护。

② TCP/IP 管理　TCP/IP 协议中的 IP 地址管理主要指 TCP/IP 协议的安装、配置和 IP 地址的分配与管理。这部分内容将在第 7 章中作介绍。

③ Windows NT 网络的组织和用户管理　除了对域和用户进行规划、设计与实施工作外，还包括大量的日常维护工作。例如，域模式的选择、设计和实施；域用户的管理（网络用户和用户策略的建立和访问权限的分配）；利用“组”来管理用户等。

④ 文件系统管理　包括 NT 网络的文件系统的管理，资源管理器以及磁盘的管理等基本内容。

⑤ 数据保护和系统恢复　主要指系统重要数据的备份制度的建立和实施、容错技术的使用以及数据保护措施等，例如，系统数据的紧急备份和恢复手段。

⑥ 使用管理工具管理 Windows NT 网络　主要是指如何使用和管理向导工具、服务器管理器、事件查看器、性能监视器、网络客户管理器和 Windows NT 诊断器等，系统内置的管理工具对 Windows NT 网络进行综合管理。

⑦ 服务管理　主要指开始、停止和暂停系统的各项服务。

⑧ 安全管理　主要包括 NT 网络的安全基础、安全访问控制机制和网络的安全配置等几项基本内容。需要解决的基本问题为，网络访问控制、文件共享控制和安全的具体措施。

⑨ 使用命令行进行管理　对于 DOS 客户机来说，使用命令行管理是必不可少的，例如，各种 DOS 客户机与 NT Server 互联时，使用的一组 NET 命令。

上述内容中①～④为初始建立、维护和管理一个用 Windows NT 建立的 Intranet 必不可少的部分，也是 Intranet 管理最基本的内容。

至此，简单地介绍了一个使用 Windows NT 组建和管理的 Intranet 的组成，以及它的内部网络实体的设计和施工过程。在本书以后各章中，将以目前流行的网络操作系统 Windows NT 4.0 为例，来说明完成上述网络管理任务的具体方法和实现技术。

习题

1. 问答题

(1) 简述 Intranet 的基本组成？Intranet 应具备哪些基本功能？

(2) 规划和建设中小型 Intranet 的过程有哪些主要步骤?

(3) Intranet 物理网络的硬件结构如何? 包括哪些部件? 各自的功能是什么?

(4) 在进行 Intranet 内部局域网的设计时,应考虑哪些基本因素?

(5) 常用的网络系统模式有哪几种? 本章中使用 Windows NT 组建 Intranet 时,使用的是哪种网络模式?

(6) 常见的网络操作系统分为几类? 各有什么特点? 适用于什么场合?

(7) 应当如何选择网络操作系统? 中小型单位对网络安全性能要求不高时,适合选择什么网络操作系统?

(8) 对系统稳定性、安全性和可靠性要求较高的大型企事业单位,适合使用何种操作系统?

(9) 什么是 DNS 域名服务子系统? 它有什么作用?

(10) 什么是 WWW 服务子系统? 它有什么作用?

(11) Intranet 中有哪些基本的网络服务子系统? 它们的功能各是什么?

(12) Intranet 中实现网络服务子系统的服务器和客户机使用的软件有哪些?

(13) 应当怎样选择 Internet 接入服务和方式?

(14) 构建和实施 Intranet 的主要步骤有哪几步?

(15) Windows NT 网络管理的主要目标是什么? NT 网络管理的具体内容有哪些?

2. 设计和应用题

按照网络系统集成的方法、原则和步骤规划和设计如下的小型 Intranet。

(1) 条件与设计要求。

- 30 台 Pentium Ⅲ 微机。
- 各服务器要求在任何时刻均满足 100Mb/s 传输速率的要求。
- 15 个内部用户能够安全和流畅地访问 Internet。
- 远程工作站可以在任何时间访问邮件服务器和 WWW 服务器。
- 提供必要的安全保证,保证网络中的数据资源不受非法用户的访问。

(2) 解题要求。

写出上述网络的规划设计技术文档,至少包括以下内容:

- 画出所设计的网络系统硬件结构图,标明干线和支线传输介质的型号和类型。
- 列出所选择的硬件设备的清单(类型、型号和数量)。
- 写出结构化综合布线系统的要求。
- 选择网络的操作系统。
- 写出各服务子系统的功能。
- 写出主要服务子系统的名称,并写出所需的服务器和客户端选用的软件。
- 选定邮电部门提供的合适的服务及相应的接入设备。
- 指明所需要的应用软件的名称。
- 提供网络经费预算清单,含初期投资、开发应用和维持系统的费用清单。

• 施工工期的安排。

实训题目

在上述设计和应用题中的小型 Intranet 设计的基础上，架设一个 10/100Base-T 交换式(共享式)集线器为局域网核心的小规模的 Intranet。



第6章 Windows NT 网络系统的设计、安装与配置

网络操作系统的安装主要是指其主控服务器软件平台的安装，这也是组建和管理 Intranet 或其他网络的起始和关键性工作。NT 网络系统的安装就是让系统所设计的主域控制器(PDC)正常运行起来，并完成它所负责的日常维护与管理工作，以保证信息高速公路的畅通。

主要内容：

- Windows NT 网络系统的建设；
- Windows NT 4.0 概述；
- Windows NT 网络基本模型的确定；
- 文件系统的选择；
- 网络适配器的连接、设置和诊断；
- Windows NT 安装方式的选择及安装前的准备；
- Windows NT 服务器安装的基本操作；
- Windows NT 卸载的基本操作。

6.1 Windows NT 网络系统的建设

组建 Windows NT 网络时，并不是在毫无计划的状态下，进行简单的安装和配置，而需要进行精心的设计和考虑，在进行 NT 网络系统建设时需要考虑的主要问题如下：

① Windows NT 网络模型和组织方式的选择和确定；

② 系统文件格式的选择；

③ 网络主控服务器和客户工作站的安装和配置；

④ 网络各服务子系统的安装、配置和实现；

⑤ 网络中的数据保护；

⑥ 网络安全技术的选择和实现。

6.2 Windows NT 4.0 概述

1. Windows NT 网络的功能特点

Windows NT 4.0 版除了保留原有版本的特点外，还增加了许多新的功能，它的基本特点可归纳如下：

- “抢先式”多任务工作方式；
- 硬件兼容性较强；
- 先进的容错性能；
- Windows NT 4.0 具有软件的高易用性能、丰富的软件支持和高兼容性；
- 易于使用与管理的网络打印；
- 集中式的远程管理；
- 实用的管理者向导(administrator wizard)；
- 丰富的内置网络管理工具，提供多种类型的网络服务；
- 网络活动的记录与追踪；
- 一次登录即可访问多个网络资源；
- 内置的 Internet 和 Intranet 网络功能；
- 强大的用户管理功能。

2. Windows NT 的产品分类

Windows NT 4.0 是一种在网络环境下工作的多功能操作系统，其工作模式为 C/S (client/server)主从结构。Microsoft 将 Windows NT 操作系统分为 4 类产品：

- Windows NT Server 4.0(NT Server)中文版；
- Windows NT workstation 4.0(NT Workstation)中文版；
- Windows NT Server Edition；
- Windows Back Office Small Business Server 4.0。

在安装 Windows NT Server 之前，首先应当考虑选择什么样的 NT 模型，即以何种方式来规划和组织 NT 网络。

6.3 Windows NT 网络基本模型的确定

网络管理员若想管理好一个 Windows NT 网络，首先必须根据本单位网络需求的实际情况，进行组织结构的规划和设计，只有将网络结构设计好，再加上必要的网络管理，才可能使得网络安全、可靠、高效地运行。

Windows NT 网络模型是指用 NT 系统组成网络时，所对应的网络规模和组织形式。不同的 NT 网络模型，分别对应着不同的目录数据库和目录服务。由于 Windows NT 网络的网络模型有“域”和“工作组”两种。因此，确定 NT 网络模型是组建 NT 网络的起始工作。

6.3.1 目录数据库(NTDB)和目录服务(NTDS)

在目前流行的现代化网络操作系统中,大都利用一个称为目录数据库的数据库来保存用户、组和安全设置等方面的信息。Windows NT 系统中的目录数据库(NT directory data base,NTDB)包含了 NT 中的用户账户(ID)、密码、访问权限和组账户等系统的安全策略设置信息。在 Windows NT Server 中,有一个 SAM 文件(即安全账号管理器)存储着域中的所有安全机制和用户的账户信息。

Windows NT 目录服务(NTDS,NT Directory Service)是 Windows NT Server 提供的基本服务之一,NT 中的"目录服务功能"使得网络的管理更加简单,NT 中"目录服务"的目标是"一个用户,一个账户"(one uSER one sccount)。在 NT 的域管理模式下,经过信任关系的设置,使域中的每一个用户,可以使用同一个账户和密码,在相同或不同的域中登录,并使用其中的资源。因此,NT 的目录服务主要指在域模式下的目录服务功能,它更加符合现代化网络管理的要求。

NT 的目录服务(NTDS)建立在一个安全的目录数据库(NTDB)下,根据网络组织方式的不同,NT 网络中有以下两种数据库结构:

1. 在"工作组"网络模式下的目录服务功能

在工作组模式下,NT 目录服务功能(NTDS)为本地(计算机本机)的目录数据库。此时,NTDB 仅仅包括本地计算机上创建的账户和组的信息,而且这些账户和组也只能在本地使用,由本地的目录数据库进行验证。

2. 在"域"网络模式下的目录服务功能

按"域"方式组织的 NT 网络,在它的"主域控制器"(PDC)上有一个全域集中的目录数据库(NTDB),它包含了域中所有的用户账户和组的信息,这个目录数据库可以被域中的所有计算机使用。因此,只要是一个合法的域用户,就可以在域中的任何一台计算机上登录。而用户的登录身份将在 PDC 或 BDC 上的目录数据库中进行验证。

目录数据库是整个网络系统中不可缺少的重要组成部分,它用来存放域中所有的安全性数据与用户账户等信息。用户登录时,用它来核对、验证用户键入的数据是否符合其相应的身份和使用权限。由此可见,目录数据库是非常重要的,它被放在 PDC(主域控制器)上。基于目录数据库的重要性,为了保险起见,通常在网络中设置有 BDC(备份域控制器),BDC 会按照一定的规律和时间间隔保存它的备份。

6.3.2 NT 网络中"域"的概念

1. **"域"(domain)的定义**

在 Windows NT 服务器的目录环境中,"域"是一个共享目录数据库的计算机和用户的集合,通过这个共享的目录数据库,可以对域中的账户、优先权、安全性和网络资源等进行集中管理,因此,"域"是安全与集中管理的最基本单位。对于域,有多种工作模式可以进行选择和设计,请参见第 8 章的有关内容。

"域"模式的实际网络结构如图 6-1 所示。一个"域"可以包含一个或多个 NT 服务器,而一个 NT 网络可以由一个或多个"域"组成。每个"域"都拥有一台称为主域控制器

(PDC)的计算机,该计算机应是一台运行 Windows NT Server 4.0 的服务器。

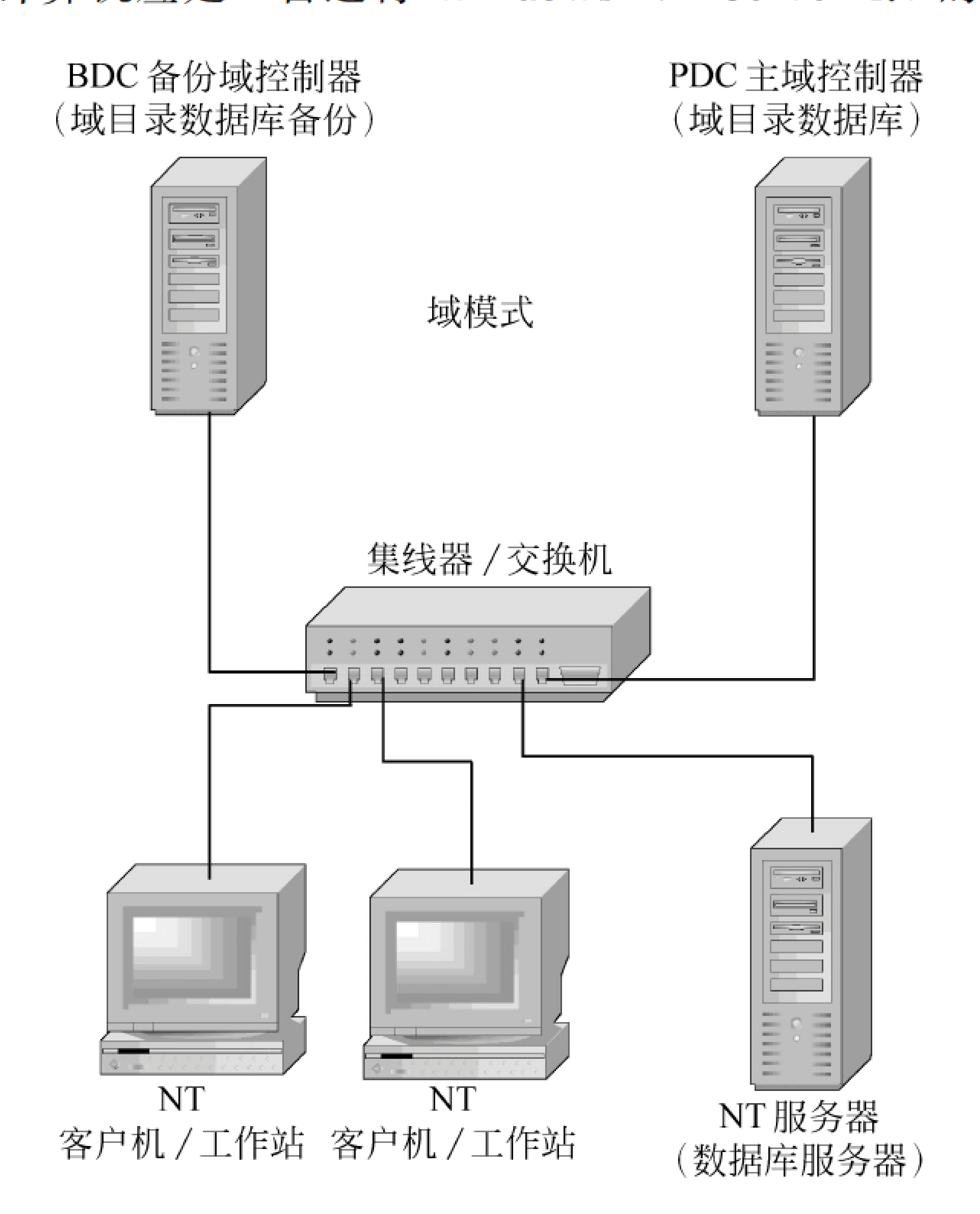


图 6-1　域的组成

"域"是由许多网络服务器与工作站连接而成的计算机群组,这个群组的成员可以使用相同的系统设定、账户系统和共享资源。使用域资源的用户,无须在每台计算机上分别建立账户,并登录到资源所在的计算机上,而只要登录到该"域",就可以共享该域中所有允许访问的共享资源。在同一"域"上的工作站或服务器,无论是在近程的较小区域内(通过传输介质连接),还是在远程的范围内,只要被定义在相同的域,彼此之间就是有关联的"伙伴",就可以享用域中的资源。例如,域用户可以通过 ISDN、PSTN 等拨号网络,从远程区域访问"域"中的资源。

2. "域"中计算机的分类

在域中安装 NT Server 软件时,可以选择的计算机身份有以下 3 种类型,它们之间是一种不平等关系。

(1) PDC(主域控制器)

PDC 是一个"域"中的主人,它包括了一个"域"中用户和组的所有信息,以及"域"的安全策略设置,是域中目录数据库的原始拷贝所在地。PDC 主要用于创建域用户,维护域的安全策略,并用于验证用户的登录。任何关于用户账户、组账户信息的改变,以及安全策略的改变都应该反映到 PDC 上才会生效。PDC 是一个域中安装的第一台计算机,需要时,PDC 可以降级为 BDC,同时提升 BDC 为 PDC。

(2) BDC(备份域控制器)

BDC 维护着一个"域"的用户和组的信息,并且保存有"域"的安全策略设置的拷贝。

PDC 定期地将目录数据库的信息拷贝到 BDC 上。BDC 的作用主要是协助 PDC 进行登录验证,分担 PDC 的工作,减轻网络流量。当 PDC 关机出现故障时,BDC 可以提升成为 PDC。

(3) 成员服务器(member server)

一般将已加入域的 NT Server 计算机称为"成员服务器",而将未加入域的 NT Server 计算机称为"独立服务器"。由于成员服务器本身并不存储域的目录数据库,也不存储目录数据库的备份数据,因此,它不参与域用户的管理工作,不能用于验证域用户。它主要用作专用服务器,例如,文件服务器、打印服务器、SQL 服务器和 RAS 服务器等。不经重新安装,普通的 NT Server 计算机不能提升为 PDC 或 BDC。

3. 采用"域"模式的特点

(1) 集中的账户管理

在一个域中,所有用户账户的管理和整个网络的安全策略都可以在"单个点"上进行,即在 PDC 上进行集中管理。

(2) 资源的集中管理

域中的资源是分散在域中的每台计算机上的,这些资源除了能够由每台计算机的管理员管理外,还能够由域管理员在一点进行集中管理。他们不但可以利用系统自动建立的隐含共享目录 C$ 和 D$ 进行管理,还可以给资源分配 permission(访问权限),指定 audit(审核)规则。

(3) Profile 文件跟随用户而走动

在域中,域的管理员能给用户指定一个基于服务器的 profile 文件,该文件存储在"主域控制器"上,经设置后,用户对环境配置所作的变化都会存储到"主域控制器"上,因此,无论用户从域中的任何一台计算机上登录,都能看到自己所熟悉的工作环境。

(4) 资源访问非常方便

任何一个合法的域用户,登录到"域"以后,就能够访问域中任何一台计算机中该用户具有授权许可的共享资源。

4. 用户权限和用户账号

(1) 用户账号

当某一用户需要登录上网时,必须向管理员申请一个用户的账号,以后每次上网时,必须首先输入用户名,再输入密码(即口令),经验证合格后,才可以进入网络。

(2) 用户权限

在域的系统中,用户存取数据与使用共享资源必须依据所拥有的权限来进行,这样,才能够保障系统的安全性。所以,每一个用户只有获得了域管理者授予的操作权限,才能以此权限存取数据或使用共享资源。

综上所述,域的概念是实现 NT 目录服务目标"一个用户,一个账号"的基础。

6.3.3 NT 网络中"工作组"的概念

1. "工作组"(workgroup)的定义

工作组是一组由网络连接而成的计算机群组。在 Windows NT 中用户也可以将网

络组织成“工作组”的方式，其网络结构如图 6-2 所示。与域中的集中式管理方式截然不同的是：工作组模式下的资源和账户管理是分散在网络中的各个计算机上的。在工作组方式中的每一台计算机的地位是平等的。例如：每一台装有 NT Workstation 的计算机上都有自己的目录数据库，因此，每台计算机的本地管理员分别管理自己的目录数据库，即管理自己建立的用户账号和其他安全信息，经过适当的权限设置后，也可以实现资源共享。由于工作组中的计算机账号是由各自的管理员分别建立和管理的，因此当计算机的数目过多时，会造成管理工作量的增加。所以，这种组织方式适用于不超过 10 台计算机的小型对等网络。

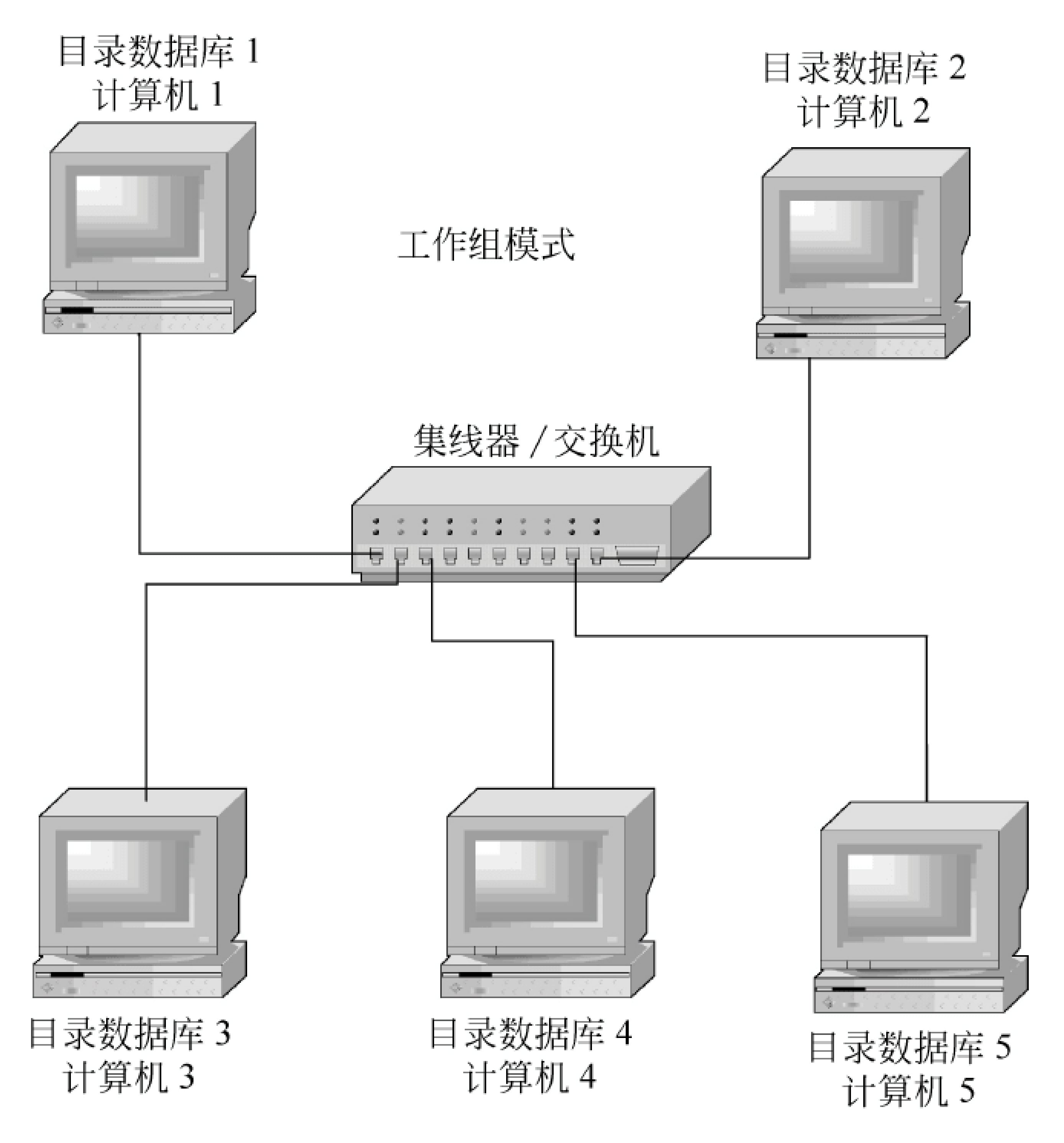


图 6-2 “工作组”的组成

2. 采用“工作组”模式的特点

工作组方式与域模型的工作方式相比，其特点如下所述：

① 工作组中的所有计算机之间是一种平等的关系，没有主从之分。

② 工作组模式下资源和账户的管理是分散的。每台计算机上的管理员能够完全实现对自己计算机上的资源与账户的管理。

③ “人机不分开”，每台计算机上都有一套目录数据库，用以验证在自己计算机上所创建的本地用户，一个用户只能在为他创建了账户的计算机上登录，并由该计算机上的目录数据库来对他的身份进行验证。

④ 用户的“配置(profile)文件不跟随用户走”，不经用户的特殊设置，用户从不同的计算机上登录之后，一般不会拥有相同的工作环境。

⑤ 工作组模式下，资源的管理是分散的，因此，只有通过以下途径才能实现资源的互相访问：

- 利用 guest 账户访问，即取消原来该账户的“禁用”属性，当登录资源计算机或联接到目的资源上的时候，如果提示输入该账户和密码，请输入 Guest 及相应的密码。
- 在目的(资源)计算机上为使用资源的用户创建一个账户，当登录资源计算机或联接到目的资源上的时候，如果提示输入该账户和密码，请输入所创建的账户名及相应的密码。

工作组的模式的缺点是，当用户账户数量较大时，管理工作量较大，管理不方便，并且不能进行资源和账户的集中管理。

综上，对于企事业单位的 Intranet 系统来说，一般都选择 NT 的“域”模型方式，只有要求不高的小型办公室网络才会选择 NT 的“工作组”模型方式。

6.4 文件系统的选择

在传统的 DOS、Windows 95/98 操作系统中，目录和文件的磁盘分区记录都是由文件分配表 FAT(file allocation table)进行统一管理、分配和控制的。因此，在建设 NT 网络之前，另一件重要的工作就是选择和确定拟安装 NT Server 或 NT Workstation 软件的计算机的文件系统格式。选择之后，即可开始安装 NT Server。

1. NTFS 文件系统的主要特点

Windows NT 也是一种操作系统的软件，它的文件系统格式为 NTFS(NT file system)格式。它与 Windows 95/98 相比的一个最大的不同之处就是 Windows NT 提供了 NTFS(NT file system)文件系统，其主要特点如下所述：

① 自动存储文件信息的记录。

在 NTFS 文件系统中，用来记录文件信息的 MFT(master file table)会自动存储备份。因此，当磁盘发生故障时，可以使用备份文件恢复文件的配置信息。

② 在 NT 中磁盘空间的限制。

- 使用 FAT 文件系统时，文件和分区的最大值为 4GB(2^{32}字节)；
- 使用 NTFS 文件系统时，文件和分区的最大理论值为 16EB(2^{64}字节)。但是，受到硬件和其他因素的限制，在实际运用时达不到理论值的标准。

③ 支持长文件名。

④ 支持文件级的权限设置。

2. 选择 NTFS(NT file system)文件系统的理由

① 网络中仅使用 Windows NT 网络操作系统。

② 系统要求文件级的安全性。例如，需要对文件和目录进行权限管理。

③ 系统对本地安全性要求较高。

④ 需要 NT 文件的压缩。

⑤ 需要对本机发生的事件进行跟踪记录。

⑥ 需要利用 Macintosh(苹果机)的文件共享服务。

⑦ 需要从一个 Novell NetWare Server 服务器上迁移目录和文件。

3. 选择 FAT(file allocation table)文件系统的理由

① 若希望 Windows NT 与 Windows 95/98/Me 或 MS-DOS 实现多引导,则应使用 FAT 分区作为系统分区。这种情况下,C 盘必须格式化为 FAT 格式。

② 在基于 RISC 机型上计算机安装 Windows NT,系统分区至少是 2GB 的 FAT 分区。

③ 需要保留原有系统及其应用时,应使用 FAT 文件系统。

6.5 安装和配置 Windows NT 计算机

在服务器和工作站上安装和配置 NT Server 与 NT Workstation 软件的过程十分类似,本节主要介绍 NT Server 的安装步骤,安装 NT Workstation 时,用户可以参照进行。

6.5.1 选择安装 Windows NT 软件的服务器和工作站

在 Windows NT 软件安装之前应当确定以下问题:

1. 检查拟安装的 NT 服务器和工作站的硬件

为了顺利地安装 NT,在安装之前,除了检查计算机的基本配置是否满足要求外,还应该检查计算机的所有硬件是否具有支持 Windows NT 的硬件驱动程序。首先检查 NT 的硬件列表(HCL),该列表列出了 NT 支持的所有设备,如果某个设备不在其中,则应与生产该设备的硬件厂商联系,请他们提供 Windows NT 的驱动程序。例如,安装服务器显卡、SCSI 接口的硬盘、CD-ROM 驱动器和软盘驱动器等其他设备。

2. NT 局域网常见工作站

对于不同工作站,硬件的需求有所不同,因此,应根据需要进行调整和配置。常用工作站可分为几类:文件处理工作站、排版系统工作站、计算机辅助设计/制造绘图工作站和支持决策系统的工作站等。

6.5.2 网络适配器的连接、设置和诊断

网卡(network adapter card),或者简称为 NIC(network interface card)。它是计算机与网络上其他计算机通信的最基本的硬件设备。网卡通过“网线”,即网络传输介质,例如:同轴电缆、双绞线等与其他计算机连接。

1. 安装网卡驱动程序

安装网卡的硬件之后,一个非常重要的工作就是正确安装和配置网卡驱动程序。每个网卡通常配有一个网卡驱动程序,利用此程序可以控制网卡的运行。不同的网卡配有不同的驱动程序,常见的网卡类型有:NE2000(16 位 ISA)兼容卡、Realtek(32 位 PCI)、3COM、D-Link 等网卡。

ISA 网卡的原始驱动程序常常是在 DOS 下运行的一组实用程序。下面以常见的 NE2000 网卡为例,说明网卡驱动程序的安装及检测过程。将网卡驱动程序磁盘插入软

盘驱动器,并键入 a:\UTITITY\setup.exe 命令,激活如图 6-3 所示窗口。

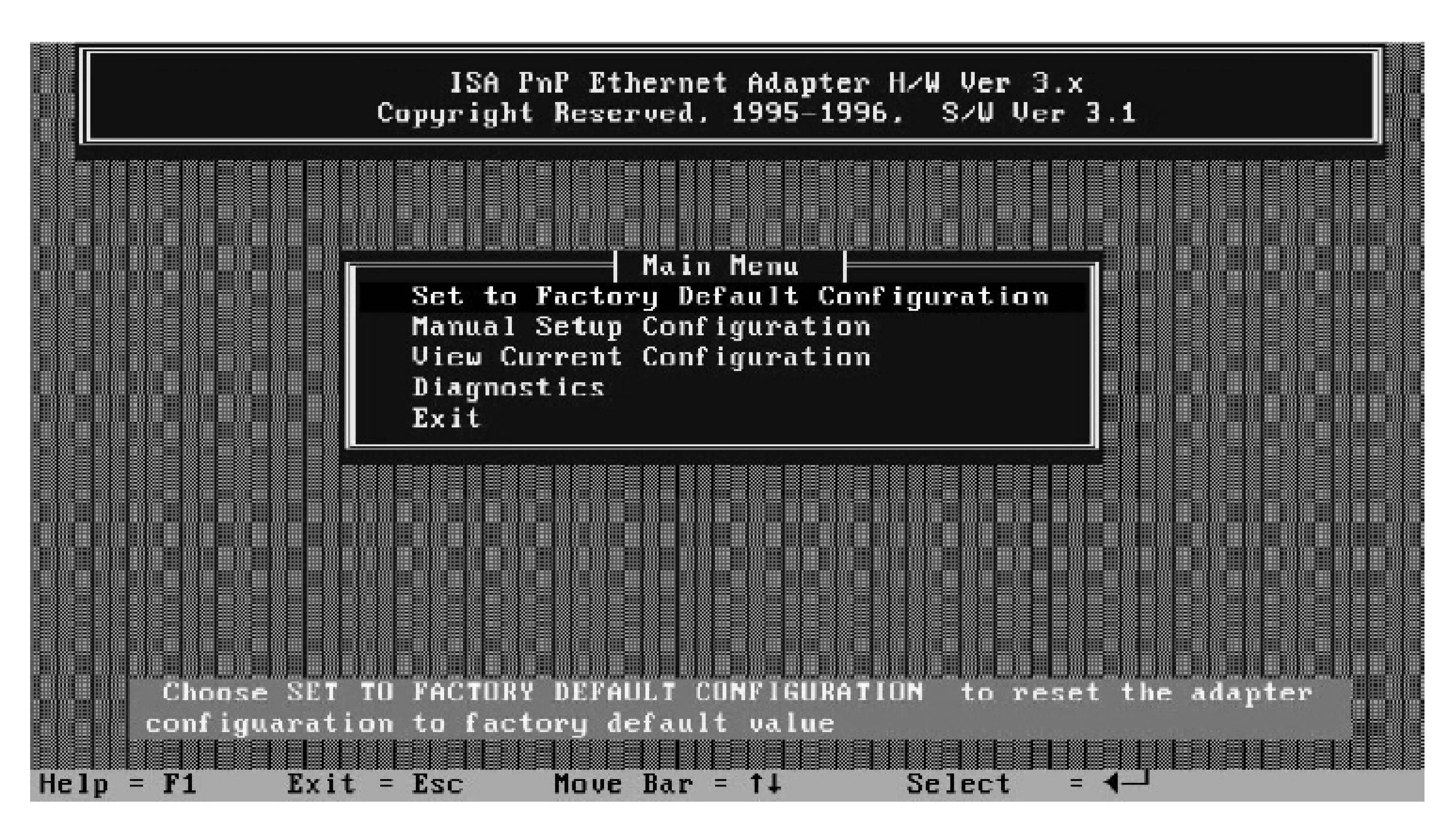


图 6-3 网卡设置、检测菜单窗口

2. 设置和诊断网卡(NIC)

这组程序运行时,一般除了配置网卡的 IRQ 和 I/O 地址之外,还可以进行简单的网络测试。运行网卡驱动程序的步骤如下:

① 在 DOS 启动方式下,运行 A 盘的 setup.exe 程序,将激活如图 6-3 所示的网卡设置、检测菜单窗口。

② 在图 6-3 所示窗口中,首先选择 Manual Setup Configuration(手动设置)选项,激活图 6-4 所示的网卡参数设置窗口,在此窗口中应对"I/O 地址"和 IRQ 等参数进行设置。例如:此计算机的 I/O 地址设为"300",IRQ 设为"11"等。设置时应当注意这两个参数不应与本机内其他硬件使用的参数相同。

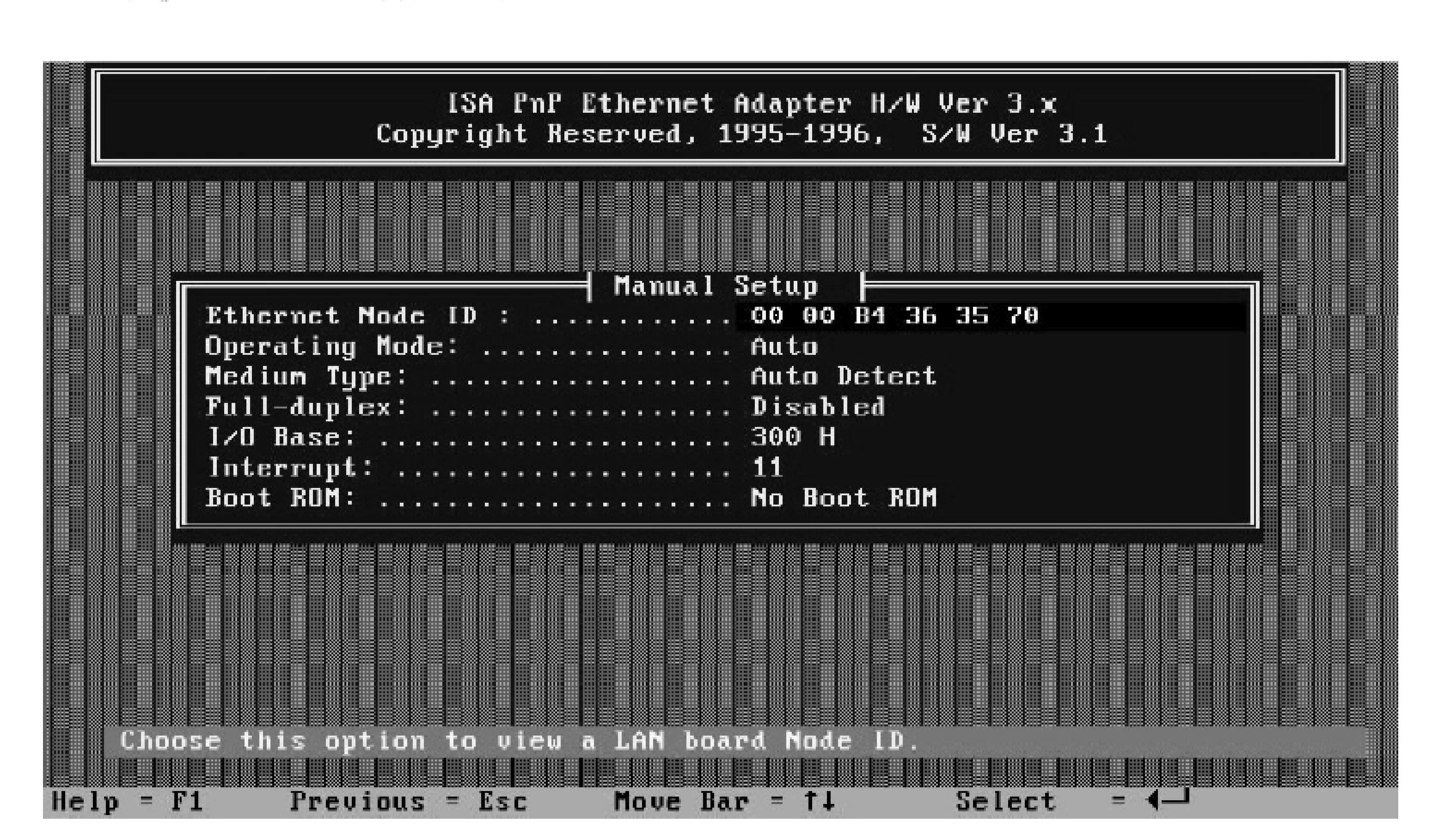


图 6-4 网卡参数设置窗口

③ 在图 6-4 所示窗口中,将网卡参数设置好之后,按 Esc 键返回如图 6-3 所示窗口。选择 Diagnostics(诊断)选项,激活如图 6-5 所示的 Diagnostics(动态诊断)窗口。

④ 如果图 6-5 所示的 Fail Count(失败记数)中的各项全为 0,则说明此网卡工作正常;否则说明网卡的工作不正常,可根据界面的提示检查网络中的有关硬件及其相关的设置参数。根据笔者经验,如果是 16 位的 ISA 网卡,为了避免安装 Windows NT 网络中出现麻烦,在正式安装 Windows NT Server 或工作站端的网络连接软件之前,应首先在

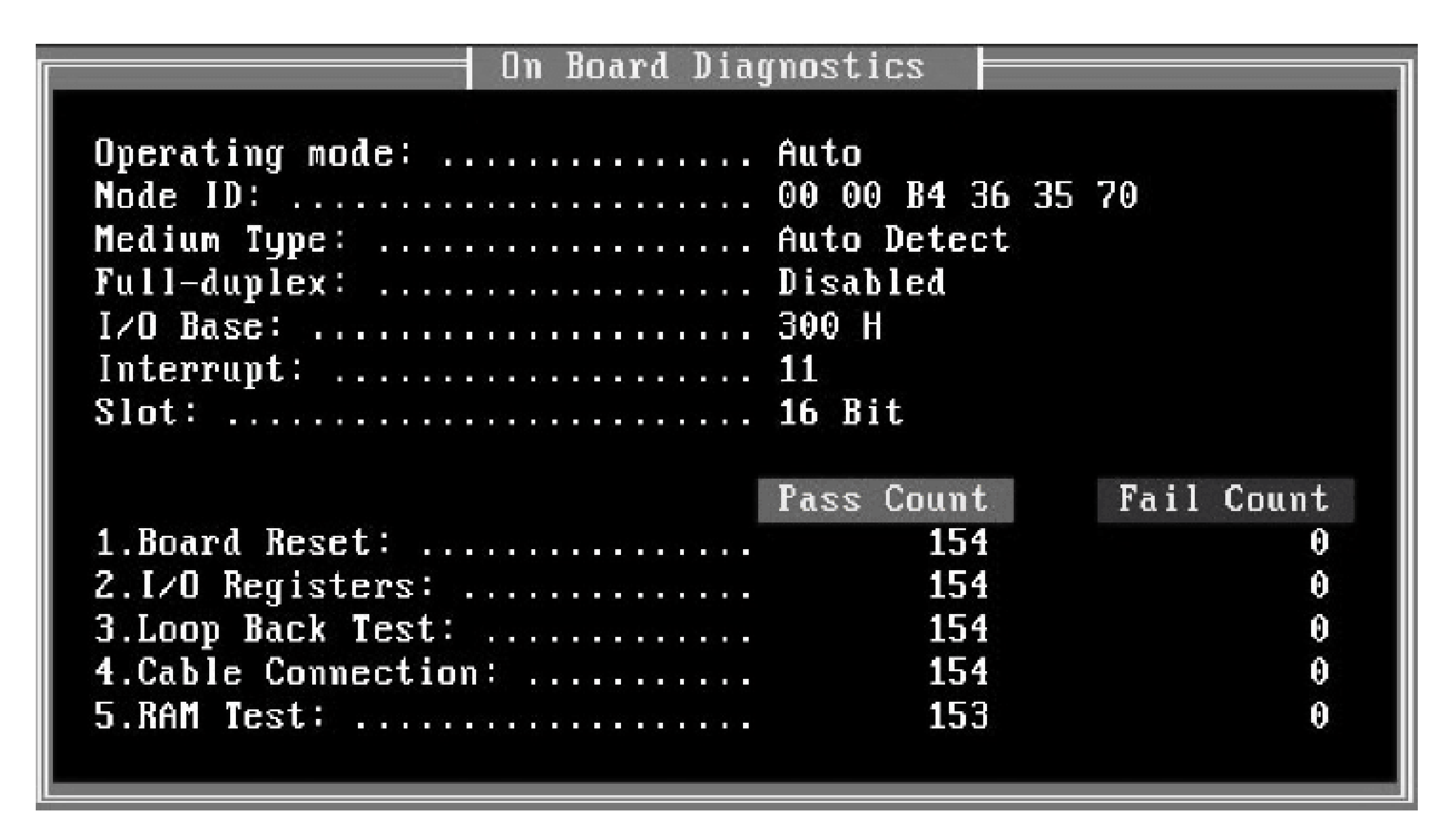


图 6-5　Diagnostics(动态诊断)窗口

DOS 下设置好网卡上的硬件参数的配置,并把它记录在案以备查询。现将这些参数简述如下:

- IRQ(interrupt request)硬件的中断请求　要求不能和本机上其他硬件使用的 IRQ 值冲突,否则网卡不能正常工作,造成网络不通。
- I/O 地址(I/O address)　要求不能和本机上的其他硬件冲突,否则也会引起网卡工作异常,网络不通。
- 网卡上的 BOOT ROM 地址　请注意不要使用与其他设备相同的地址,否则 BOOT ROM 将无法正常工作。
- DMA(直接存取存储器)　设置网卡上的 DMA CHANNEL,如果网卡上没有用 DMA,则不需要设置。

6.5.3　Windows NT 安装方式的选择及安装前的准备

1. NT 网络的最低硬件要求

为了顺利安装 NT,在安装之前,必须再次检查计算机的所有硬件是否符合安装的最小硬件条件,同时核对是否具有各种硬件的 NT 驱动程序。如果没有,则应向生产该设备的硬件厂商联系,请他们提供支持 Windows NT 的驱动程序。

2. 选择 NT 网络的安装方式

NT Server 或 NT Workstation 都可以通过软盘、CD-ROM(光盘)、硬盘或网络等媒介进行安装。下面就各种安装方法的要点做简单介绍:

(1) 软盘-光盘安装

软盘-光盘安装的速度较慢,但方法简单。软盘-光盘安装的步骤如下:

① 先从软盘启动系统,例如 DOS 启动盘、Windows 95/98 等。

② 使用 FDISK 划分 DOS 磁盘分区(FAT16),也可以使用其他软件划分分区。

③ 格式化引导磁盘,例如,使用 DOS 命令“format C:/s”格式化 C 盘。

④ 安装启动光盘,进入 CD-ROM,使用 Windows 98 启动盘也可以启动光盘。

⑤ 转入名为 NT Server 或 NT Workstation 盘的 I386 安装目录。

说明:启动安装程序之前,有时必须先使用锁定程序锁定安装磁盘,才能正常安装。

例如：在 DOS 下输入“lock c:”或“lock d:”可以锁定指定磁盘。

⑥ 输入 NT Server 或 NT Workstation 的安装启动命令 winnt.exe/b，进入安装进程。

(2) 软盘-硬盘-光盘安装

软盘-硬盘-光盘安装是指如果硬盘足够大，可以先将 NT Server 或 NT Workstation 光盘上的所有安装文件拷贝到本地计算机上的某个目录下，再进行安装，这种方法的安装速度较快。软盘-硬盘-光盘安装的步骤如下：

① 先从软盘启动。

② 使用 FDISK 划分 DOS 磁盘分区(FAT16)。

③ 格式化引导磁盘。

④ 安装并启动光盘，进入 CD-ROM。

⑤ 将光盘中名为 I386 的安装目录，全部复制到硬盘上。

⑥ 转入 I386 目录，说明同上。

⑦ 输入 Windows NT 的安装启动命令 winnt.exe /b，进入安装进程。

(3) 硬盘直接安装

当硬盘足够大时，可以采用硬盘直接安装方式。即先从对等网上的其他计算机上复制安装文件到计算机的本地硬盘上的某个目录下，再进行安装。例如：可以利用 DOS 或 Windows 95/98 组建的对等网进行系统安装文件的复制。这种方法适用于大量计算机的安装，但是如果大量计算机同时使用共享式集线器进行文件传输时，则速度较慢，会影响到安装速度。硬盘直接安装的步骤如下：

① 在对等网中，先连入某个文件服务器上。

② 复制上面 NT Server 或 NT Workstation 的 I386 安装目录到 FAT 格式的本地硬盘。

③ 转入本地的 I386 目录。

④ 输入 Windows NT 的安装启动命令 winnt.exe /b，进入安装进程。

(4) 光盘(CD-ROM)直接安装

方法 1：

在安装少量的计算机时，可采用从光盘直接安装的方法，例如：网络服务器就可以采用光盘安装的方法。自动安装步骤如下：

① 启动 FAT 系统文件分区格式的 Windows 95/98 系统。

② 插入安装光盘。

③ 进入自动安装过程。

方法 2：

在 FAT 格式的 Windows 95/98 系统下，安装少量的计算机时，可采用命令安装启动 CD-ROM 的方法，其步骤如下：

① 启动 FAT 系统文件分区格式的 Windows 95/98。

② 插入安装光盘。

③ 选择“开始”→“运行”命令，在打开的窗口中输入安装启动命令 winnt.exe /b，进入

安装过程。

方法 3：

在 Windows NT 系统下，采用命令方式，安装启动的步骤如下：

① 启动 NTFS 系统文件分区格式的 NT Server 或 NT Workstation 系统。

② 插入安装光盘。

③ 选择“开始”→“运行”命令，在打开的窗口中输入安装启动命令 winnt32.exe/b 进入安装过程。

(5) 网络直接安装

如果网络的传输速度较快，则通过网络安装就是一种较快的方法。当要对大量的计算机进行安装时，应采用网络安装方式。例如，企业网络中 NT Workstation 的安装。采用网络安装的步骤如下：

① 将 NT 的安装文件拷贝到一个文件服务器上的某个目录下，例如：NT Server 或 NT Workstation 目录，并将该目录设为共享。

② 在需要安装 NT 软件的计算机上，应安装有 DOS 或其他的联网软件，用以连到上述的文件服务器上。

③ 接通网络。

④ 使用刚才共享目录中的 NT 软件进行安装。例如转入共享目录 I386。

⑤ 输入安装启动命令 winnt.exe /b 后，进入安装过程。

(6) 硬盘克隆安装(*)

当需要对大量同类型的计算机进行安装时，有时采用硬盘克隆的方法。即按照上面的任何一种方法做好一台计算机，然后使用硬盘的某种克隆软件克隆该硬盘的映像文件。之后，使用该硬盘的映像文件克隆所有其他计算机上的硬盘，从而实现快速安装和配置的目的。注意，克隆安装的方法适合于一般应用软件和 NT Workstation、Windows 95/98 等操作系统的快速安装，而不适用于多台 PDC 或 BDC 上的 NT Server 软件的安装。

(7) 硬盘保护卡安装(*)

如果有条件购置“硬盘保护卡”，则可采用硬盘保护卡来安装和维护网络。这种方法无疑是一种较好的方法。如果网络的传输速度较快，例如：使用 10/100Mb/s 的交换机，则完成整个计算机房的安装比安装两台计算机所需的时间还少。但必须同时提醒用户注意的是，加装硬盘保护卡之后，系统运行的速度会明显降低。有时还会影响到各种操作系统的功能。

在实验室或网吧中，通常具有大量同类型的计算机，而且其安装和日常管理工作较为复杂。此时如果为每台计算机花费 150～250 元购置硬盘保护卡，必定会取得良好的管理和维护的效果。硬盘保护卡安装的安装步骤如下：

① 逐台安装好硬盘保护卡、网卡和传输介质。

② 规划并安装好一台计算机的所有软件。

③ 将安装好的计算机设置为发射台。

④ 将其他未安装的计算机设置为接收台。

⑤ 使用发射台上的发射传输功能，将规划和安装好的系统同时发送、传输到所有的

接收端计算机上。

⑥ 传输完毕之后，需要对每台计算机的特殊参数逐一修改，例如：有关 IP 地址、计算机名等信息。

⑦ 以后，每台计算机上的硬盘保护卡将会按规划的时间间隔自动保护每台计算机的硬盘内容。例如，每次启动恢复、每日恢复原来系统的内容等。

说明：标注有(*)的方法不但可以快速安装网络，还可以快速恢复网络中的每台计算机。

6.5.4 Windows NT 安装的基本操作

1. 安装 Windows NT 软件的准备

(1) 安装 NT 网络需要的信息

完成安装 NT Server 或 NT Workstation 的步骤类似，所需要准备的信息大体相仿，主要有如下一些信息：

① 用户的姓名和所在公司名称。

② 计算机名(例如 ZDH01)。

③ 语言(地区)和时区。

④ 选择网络适配器型号。例如 SNE2000、D-Link DE-220P Adapter 等。

⑤ 网络适配器参数设定。例如 I/O 地址为 0x300，中断请求级 IRQ 为 11 等。注意：此处设置的值应与 DOS 驱动程序下设置的相同。

⑥ 选定网络协议。例如 TCP/IP 协议、NWLink IPX/SPX 兼容传输协议和 NetBEUI 通信协议等。配置 TCP/IP 协议。应事先划分拟安装的计算机在该网络中的 IP 地址(例如 202.112.144.10)及子网掩码(例如 255.255.255.0)。

⑦ 用户计算机在域中的作用。例如，NT Server 中的 PDC、BDC 或独立服务器；NT Workstation 中无此选项。

⑧ “域”名或“工作组”的名称。例如 ZDHDOMAIN。

⑨ 管理员的口令。首次进入安装了 NT 软件的服务器或工作站时，需要输入此密码，请千万不要忘记。首次进入后，可以对此密码进行修改。

⑩ 完成安装 NT Server 的实验，在 Pentium 或 MMX 系列的计算机上大致需要两个小时左右的时间，如果计算机配置较高，所需要的时间就较短。在一般的 Pentium 计算机上完成安装 NT Workstation 的实验，大致需要 100 分钟左右。

(2) 安装环境的选择

安装 Windows NT 之前，应首先删除其他厂商的网络操作系统，例如，Novell 公司的 NetWare，否则无法顺利安装或升级。然后，选择是从 Windows NT 旧版本升级，还是全新的安装。

① 在 NT 4.0 以上的版本上安装或升级

使用 winnt.exe 或 winnt32.exe 安装命令进行安装。

- winnt.exe 可以在 FAT 格式的 DOS、Windows 95/98 环境下执行。
- winnt32.exe 可以在 NT 32 位操作系统下执行，例如 NT Workstation 上运行。

② 以前安装过 NT 4.0，现在重新安装

对于已安装过 NT 4.0 版本的用户，重新安装时，应先卸载 NT（卸载 NT 的步骤参见本章的 6.6 节），再按照本书所介绍的安装方法进行安装。

(3) 硬盘接口的选择

计算机硬盘驱动器多采用 IDE 或 SCSI 两种接口。Windows NT 在安装过程中可以检测并提供相应的驱动程序。但是，有一些 SCSI 接口不能被 Windows NT 识别，安装时应提供厂商附带的支持 NT4.0 的驱动程序。

(4) DOS、Windows 95、98 和 Windows NT 多重引导的安装

对于所安装计算机的大硬盘，当含有 DOS 的多重引导时，所划出的引导 DOS 的分区应当是一个不大于 2GB 的 FAT16 分区。

安装时，首先在 FAT16 的引导分区上安装 DOS 和 Windows 95/98；然后，从 Windows 98 中安装 Windows NT。安装之后，如果需要，可以使用其他磁盘工具(pqmagic.exe)、NT 的补丁程序，进行必要的分区合并、转换等操作。

(5) 安装 Windows NT 对大硬盘的处理

如果在安装 Windows NT 之后，出现“蓝屏”现象，这可能是由于在大硬盘上安装、启动 NT 而引起的，若系统提示 atapi.sys 驱动错误。此时，可以使用 NT 盘中的补丁程序 sp4～sp6 进行补救。方法是：先展开 sp4 或安装 sp4 到指定目录中，从该目录中找寻 atapi.sys 程序(27K)，并用该程序替换系统中临时安装目录或系统目录中的同名文件(18K)。

(6) 安装 Windows NT 过程中的注意事项

安装过程中要注意防止以下 4 个冲突：

① 在安装网卡时，在设置 I/O 地址和 IRQ 时，不能和本机上的其他硬件使用的值冲突，否则会引起网卡不能正常工作，网络不通。

② 在对 TCP/IP 协议进行配置时，应当防止 IP 地址的使用冲突，即本机所使用的 IP 地址不能与其他计算机的冲突，还要注意同一子网中使用的网络编号应当相同，否则计算机之间不能很好地通信。

③ 在安装 NT Server 作为 PDC 时，要防止域名冲突，即所设置的域名不能与其他域名相同。

④ 在安装 NT 时，要防止计算机名冲突，即所使用的计算机名不能与其他计算机使用的冲突。

(7) 安装命令的选择

如前所述，可选择光盘安装、硬盘安装或网络安装等多种方式。例如，选择硬盘安装时，从网络计算机或本地机硬盘的 I386 目录下键入安装命令：\I386\winnt.exe/b。

表 6-1 和表 6-2 列出了 winnt.exe 和 winnt32.exe 安装命令的使用格式。winnt32.exe 安装命令中的参数选项与 winnt.exe 基本相同，因此，在表 6-2 中仅列出了与表 6-1 不同的安装命令参数选项。当使用 winnt32.exe 安装命令时，参数格式可参照表 6-1 中进行。

表 6-1　winnt.exe 命令格式汇总表

winnt[/s:sourcepath][/i:inf-file][/t:drive-letter][/f][/b][/ox] [/u:script][/r:directory]	
/s:sourcepath	指定 Windows NT 系统程序的文件路径,例如 I386
/i:inf-file	指定安装信息文件,默认文件为 DOSNET.INF
/t:drive-letter	指定保存临时文件存放的磁盘,未指定时,临时文件目录为 $ WIN_NT $ ~LS
/f	制作安装磁盘时,不检验所复制的文件是否有误
/b	从硬盘直接安装,不制作安装磁盘推荐使用此方式
/ox	从 CD-ROM 上制作 3 张安装磁盘,即 setup boot disk、setup disk 2、setup disk 3
/u:script	利用设置文件 unattend.txt 自动安装
/r:directory	设定安装目录
	未使用任何参数时,则 winnt.exe 会首先制作 3 张安装磁盘,然后开始安装 Windows NT

表 6-2　winnt32.exe 命令格式汇总表

winnt32[/s:sourcepath][/i:inf-file][/t:drive-letter][/f][/b][/ox] [/u:script][/r:directory][/e:command]	
/e:command	指定安装完成后所要执行的命令

2. Windows NT 软件安装程序的启动

启动光盘程序“E:\I386\winnt.exe”,主要有以下几种方法:

① 在文件格式为 FAT16 的 Windows 95 或 Windows 98 窗口中插入光盘后,在激活的窗口中,单击“Windows NT 安装程序”按钮,激活如图 6-6 所示的窗口。

② 在 Windows 95/98 下,选择“开始→运行”命令选项,在激活的“运行”窗口中,键入“winnt.exe /b”后,单击“确定”按钮,激活图 6-6 所示的窗口。

③ 用 Windows 95/98 启动软盘(FAT16 格式)启动系统,启动 CD-ROM 后,转入光盘的 I386 目录,键入“F:\I386\winnt.exe /b”命令后,也可以激活如图 6-6 所示窗口。

④ Windows 95/98 下将光盘上的“F:\I386”目录复制到硬盘 D 下,用 DOS 盘启动系统,转入硬盘,键入“D:\I386\winnt /b”,也可以激活如图 6-6 所示窗口。

3. Windows NT 软件的安装过程

无论使用哪种安装方法,都要运行 winnt.exe 或者 winnt32.exe。启动后,即可跟随安装向导完成 Windows NT 的安装过程。安装的主要过程如下:

(1) 安装的主要内容

① 选择安装类型。安装向导提供的安装类型有典型安装、便携式安装、最小安装和定制安装(即用户自行选择设置)4 种,一般选择典型安装。

② 键入计算机和用户的有关信息。当安装 Windows NT 服务器时,还应键入该服务器所购买的版权信息。注意,计算机名称应小于 15 个字节,该名称是这台计算机在网络上的“标识符”,因此一定不要与其他的计算机名称、域名称、工作组名称等相同。

③ 选择服务器类型。安装 Windows NT 服务器软件时，应当注意选择所安装的服务器在网络上的类型。应当在 PDC（主域控制器）、BDC（备份域控制器）和独立服务器中选择一种，如果是域中的第一台计算机，则必须选择 PDC。

④ 设置系统管理员密码。在安装过程中会自动建立系统管理员（administrator）账户，该账户拥有最大的权限，用来管理系统。键入密码的长度应小于 14 个字节。请注意，此密码应被妥善保管，否则以后无法登录。

⑤ 制作系统紧急恢复磁盘。用户首次安装时，建议制作此磁盘，还应经常更新此磁盘。因为，当系统出现故障时，使用此盘和 3 张安装磁盘（即 setup boot disk、setup disk 2、setup disk 3）便可以迅速修复被损坏的系统。

⑥ 选择安装网络组件。

(2) 安装程序的主要阶段和步骤

进入自动安装的引导过程后的安装过程可以分为以下 4 个主要阶段：

第 1 阶段：

这个阶段主要完成磁盘的格式化、复制安装文件和检查硬盘等任务。

① 当出现图 6-6 所示窗口时，键入系统文件所在路径，例如，“F:\I386”，按 Enter 键，开始复制文件，复制结束后，重新启动系统。



图 6-6　确定安装路径窗口

② 系统重新启动后，在显示的“确定安装方式”窗口中，可以根据情况选择安装、修复(R)或停止安装等安装方式，例如，选择重新安装时，按 Enter 键继续。

③ 当系统显示“安装大容量存储设备”窗口时，可根据情况选择安装大容量存储设备，按 Enter 键继续。

④ 当系统显示“安装磁盘选择”窗口时，可根据需要选择 Windows NT 要安装的磁盘和文件格式，例如，选择“C:FAT”选项后，按 Enter 键继续。

⑤ 当系统提示并询问是否转换该磁盘的文件格式时，应根据需要进行选择。例如，可选择“将此磁盘(C:)分区转换为 NTFS”，或选择“保持现有文件系统”，如果对系统格式不熟悉，建议选择后者。

⑥ 选择之后，按 Enter 键继续，即可跟随安装向导的提示依次完成以后的各步骤，直到系统重新启动。

第 2 阶段：

这个阶段主要完成输入个人信息、计算机的服务器类型的选择，以及根据软件授权的许可协议对用户的数目进行选择等各项任务。

① 当系统重新启动后，当显示“许可协议方式”的选择窗口时，用户应根据所购买的使用权限进行选择。之后，单击“下一步”按钮继续。

② 当系统显示“NT 服务器类型选择”窗口时，选择所要安装的服务器类型，如果是域中的第 1 台计算机，请选择“主域控制器”。选择之后，单击“下一步”按钮继续。

③ 当询问选择是否制作紧急修复磁盘，建议选择“是”。选择之后，单击“下一步”按钮继续。

④ 当系统显示“选择安装组件”窗口时，可以选择所要安装的组件，建议根据实际需要选择。选择之后，单击“下一步”按钮继续。

⑤ 当系统显示如图 6-7 所示窗口时，选择连入网络的方式，根据实际需要选择之后，单击“下一步”按钮继续。



图 6-7　选择连入网络方式的窗口

第 3 阶段：

这个阶段主要完成网络有关的各种信息，例如，是否安装 IIS、安装和配置网卡类型、输入计算机名称和域名、选择与配置 DHCP 网络服务和安装通信协议等各项任务。

① 当询问是否安装 IIS 2.0 时，应当根据实际需要进行选择。选择之后，单击“下一步”按钮继续。

② 当系统安装过程显示“网络协议”窗口时，用户应根据实际选择需要，选择和安装网络协议，之后，单击“下一步”按钮继续。

③ 选择该计算机网卡的型号和参数设置，设定之后，单击“下一步”按钮继续。注意，对于 ISA 网卡，此处的参数值应当根据 DOS 的网卡驱动盘设置的值进行设置，否则会造成网络不通。

第 4 阶段：

这个阶段主要完成最后的安装和配置工作，例如：如果前面选择安装了 IIS，则在这个阶段可以对 IIS 服务器进行配置。另外，系统还会检查和配置系统的日期、时区、显示器

的色板、字型和桌面环境等。安装上述内容时，只需根据系统的提示进行选择或者测试，每步完成后，单击“确定”按钮，继续下面的步骤，直至最后整个系统安装完毕，系统重新启动。

(3) 安装其他外部设备

跟随安装向导完成安装之后，可能还需要安装和设置显示卡、声卡和调制解调器等其他硬件设备，直至各种硬件设备工作正常为止。在安装 Windows NT4.0 时，对于许多设备，都需要进行单独安装。安装时，一般要求提供 Windows NT 3.51 版以上的设备驱动程序和 NT 的补丁程序。例如，安装显卡时，系统常要求先安装 NT 的补丁程序 sp4～sp6，再安装设备的驱动程序。

(4) Windows NT 服务器的基本配置

① 添加和配置网络客户。

② 添加和配置网络服务。

③ 安装、配置和检测 TCP/IP 协议和其他协议(NetBEUI)。一般 PDC 和 BDC 上应安装所有工作站上用到的协议。

④ NT Server 的启动。

6.6 Windows NT 卸载的基本操作

当所安装的 NT 系统被损坏，需要重装时，应首先卸载 Windows NT，否则会出现各种意想不到的问题。Windows NT 的卸载靠单纯的删除分区或格式化是不能完成的，因为 NT 一旦安装成功，它可能已经改变了磁盘的文件格式，因此，卸载的步骤与所使用的文件系统的格式有关。

1. NT 安装在 FAT 分区上的卸载操作

如果磁盘在不同的 FAT 分区中安装有不同的操作系统时，通过下列方法可以将系统恢复为仅有 Windows 95/98 或 MS-DOS，NT 安装在 FAT 分区上的卸载操作步骤如下：

① 用 Windows 95/98(FAT16)或 MS-DOS 的系统软盘引导系统。

② 启动后，计算机进入 MS-DOS 环境，运行命令“sys c:”，将 Windows 95/98 或 MS-DOS 的系统文件传到 C 盘。

③ 取出软盘，从硬盘 C 重新引导系统。

④ 删除含有 NT 字样的目录，例如 winnt-root、Windows NT 或 winnt 和以下的 NT 文件。

⑤ 删除文件 c:\pagefile.sys、c:\boot.ini(隐含)、c:\nt *.* 和 c:\bootsect.dos(隐含)。

2. NT 安装在 NTFS 分区上的卸载操作

FDISK 不能删除 NTFS 分区，删除 NTFS 分区需利用其他软件或工具。NT 安装在 NTFS 分区上的卸载操作方法和步骤如下：

(1) 删除 NTFS 分区的第 1 种方法

① 使用 NT4.0 的第一张引导软盘启动并引导系统。如果没有这个盘,运行 winnt/ox,可以制作 setup boot disk、setup disk 2 和 setup disk 3 等 3 张磁盘。

② 当提示创建或选择一个分区时,选择欲删除的 NTFS 分区。

③ 按"D"键,即选择删除该分区。

④ 删除 NTFS 分区后,按 F3 键退出。

⑤ 使用所需要的系统引导盘引导系统后,重新创建分区。

⑥ 格式化引导分区,然后重装 Windows NT、MS-DOS、Windows95/98/2000 或其他操作系统。例如,使用 FAT16 启动盘引导,划分分区后,格式化 C 盘。

(2) 删除 NTFS 分区的第 3 种方法

① 使用 NORTON8.0 的 diskedit.exe。

② 在分区表中将 NTFS 分区的系统名称改为"未用"后退出。

③ 使用所需要的系统引导盘引导系统后,重新创建分区。

④ 格式化引导分区,然后重装 Windows NT、MS-DOS、Windows95/98 或其他操作系统。

(3) 删除 NTFS 分区的第 3 种方法

① 使用具有"磁盘魔术大师"美称的 pqmagic.exe 工具,或使用其他类似工具软件,删除 NTFS 分区。

② 使用所需要的系统引导盘引导系统后,重新创建分区。

③ 格式化引导分区,然后重装 Windows NT、MS-DOS、Windows95/98 或其他操作系统。

6.7 各种 NT 网络工作站的互联

前面介绍了 Windows NT Server 4.0 的安装和卸载的方法,而组建一个 NT 网络,除了需要安装 NT 服务器外,还要实现各种网络工作站与 NT 服务器的连接及资源共享。本节将介绍在 Windows NT 网络中,各种网络工作站的安装、配置和管理技术,这是组建一个 Windows NT 网络必不可少的部分,也是网络管理员必须熟练掌握的基本技术之一。

6.7.1 网络工作站连接前的准备

1. Windows NT 网络工作站的连接前应注意的主要问题

在 NT 网络的各种工作站连接前,应着重检查以下问题:

① 网卡和网络传输介质是否安装良好。

② DOS 环境下网卡的驱动程序是否安装、设置和诊断正确,例如,IRQ 与 I/O 值是否安装正确,DOS 下的诊断程序是否已经通过等。

③ 是否选定了网络工作模型。例如选择"域"或"工作组"方式。

④ 服务器的系统软件是否已正确安装和设置。例如 NT Server 为主域控制器。

⑤ 服务器选择了何种通信协议。例如 PDC 上是否已选定了 NetBEUI、IPX/SPX 或 TCP/IP 等协议。

⑥ 子网掩码和网络编号的分配。例如对某局域网进行静态 IP 地址管理，规划中的子网掩码为 255.255.255.0；静态分配和管理 IP 地址，从 1 号计算机开始，每台计算机的 IP 地址依次为 202.112.149.1、202.112.149.3、202.112.149.5 和 202.112.149.7 等。

2. Windows NT 网络工作站的安装步骤

根据网络工作模式的不同，应该正确选择和设置用户端。无论使用的工作站是什么，选用的工作模式是什么，工作站的设置一般都可以分为下面几个主要部分：

① 正确安装工作站的操作系统。

② 在工作站上正确安装和设置网卡。

③ 在工作站上正确安装和配置网络协议。例如：选择配置 NetBEUI、IPX/SPX 或 TCP/IP 等协议。

④ 根据网络的工作模式，设置工作站的有关资料。例如，选择域中的组管理方式；服务器端和客户机上设置的工作组名称均为 workgroup，客户机的计算机名称为 zdh01、zdh02 等。

⑤ 检查网络工作站是否已正确联网。例如，服务器端与客户机端应在网上邻居的 workgroup 中正确显示了 zdh01，如果没有，应参照有关步骤检查和设置。

⑥ 在服务器和工作站双方实现资源共享。例如：在 PDC 服务器上将硬盘 D 设置为共享，权限为“只读”，在 zdh01 上应能读取该服务器资源上的文件；同理，其他计算机也应该能使用该计算机开放的共享资源。

3. NT Server 端为 Windows 95/98/Me/NT 各种工作站登录到“域”做的设置

① 在 NT Server 端的“域用户管理器”中，分别为每个从 Windows 95/98/Me/NT 工作站登录域的用户，建立用户账号，包括用于登录验证的“用户名”和“密码”等信息。

② 为上述用户账号设置访问权限，以便按规定的权限进行登录和访问共享资源。例如：域的系统管理员在 NT Server 上的“域用户管理器”上，建立新用户账号 zdh01、zdh02 等，并将它们加入到 domain 域，还需要设置好共享资源的访问权限。

③ 有时，正常设置后计算机还不能加入到域，可以尝试在 NT Server 端的“服务器管理器”中将该计算机加入到“域”。

④ 在 NT Server 端开放服务器上的共享资源，以供从各种客户工作站登录的用户使用。

6.7.2 NT Workstation 工作站与 NT Server 的“域”方式互联

首先，按上述步骤，在 NT Server 端为 NT Workstation 客户工作站登录域做好准备。此处的 NT Workstation 客户工作站可能是安装了 NT Workstation 软件的计算机，也可能是安装了 NT Server 软件的普通服务器。下面介绍安装了 NT Workstation 的计算机在加入域时的操作步骤和设置要点，对于安装了 NT Server 工作站的客户，可以以此作为参照。

1. NT Workstation 端用户以管理员身份登录本机做好登录"域" 的准备

当 NT Workstation 客户机系统安装并重新启动后,需要检查基本信息、连接网卡,还应补充安装工作站上的其他外部设备。此外,工作站的系统工作一段时间之后,如果出现不能正常工作等状况,还需要检查和更改有关的设置参数。

注意:用户如果需要更改本机的设置,则必须在 NT Workstation 端,以本机管理员身份登录,否则系统为查看模式,不能更改设置。

(1) 注册登录

① NT Workstation 系统登录窗口为两栏时的登录过程。

当登录窗口如图 6-8 所示的(两栏)时,表示本机登录方式,使用本机的目录数据库进行登录验证。上栏的"用户名"和"密码"为本机具有管理员权限的用户名和密码。

登录信息: 请输入有效的用户名和密码。	
用户名	administrator
密码	********

图 6-8 NT Workstation 登录窗口为两栏时的注册窗口

注意:首次登录注册时,上栏"用户名"处,应输入 administrator。下栏的"密码"处,应输入系统安装过程中确定的管理员密码。

② NT Workstation 系统登录窗口为三栏时的登录过程。

当出现图 6-9 所示的三栏登录窗口时,表示该计算机用户可以登录到"域"(即可以使用非本机目录数据库进行登录的注册验证)。如果此时需要更改 NT Workstation 的本机硬件或其他网络设置信息,则应以本机管理员身份登录,否则将进入查看模式,没有修改权限。图 6-9 所示的登录注册窗口中各项的选择如下:

- 下栏　应先使用▼选择登录的区域,如果更改系统本机设置,此处应该选择 NT Workstation 本机的"计算机名",如果是登录到"域",则应选择登录域的域名。
- 上栏和中栏　其中的"用户名"和"密码"为本机中具有管理员权限的用户名和密码。例如,可使用 administrator 作为用户名,在中栏输入他的密码。

登录信息: 请输入有效的用户名和密码。	
用户名	administrator
密码	********
域	本机计算机　▼

图 6-9 NT Workstation 登录窗口为 3 栏时的注册窗口

(2) 网卡的设置

在正式联网之前,应检查该工作站的基本信息,并将已安装的网卡设置好,才能保证

该工作站正常上网运行。

(3) 安装其他外部设备

根据笔者的经验,如果所安装的硬件不在其中,则应与生产该设备的硬件厂商联系,请他们提供 Windows NT 相应的硬件驱动程序。安装硬件设备的步骤与 Windows 95/98/Me 中的类似,可参照进行。注意,有的厂商提供的设备驱动程序,需要先安装 NT 所提供的补丁程序 sp4～sp6,再安装附带的设备驱动程序。例如:显卡的安装。

(4) 选择和设置网络通信协议

计算机之间联网和通信的前提条件是选择相同的协议,因此,若想正确连接网络,应首先设置好网络通信协议。例如:选择要配置的协议 为"TCP/IP 通信协议"后,单击"属性"按钮,在激活的窗口中,选中"指定 IP 地址"单选项,并键入分配给该计算机的 IP 地址和子网掩码,最后单击"确定"按钮,完成该协议的设置过程。

2. NT Workstation 工作站加入 NT Server"域"的方法

NT Workstation 加入 NT Server"域"有多种方法,下面介绍其中的两种:

(1) NT Workstation 工作站加入"域"的第 1 种方法

仅从 NT Workstation 端设置,将 NT Workstation 工作站加入"域"的步骤如下:

① 确保 NT Workstation 的网卡和协议已经正常安装。

② 以 NT Workstation 端的本机系统管理员身份登录本机。

③ 依次选择"开始"→"设置"→"控制面板"命令选项,在打开的窗口中,双击"网络"图标,激活如图 6-10 所示的窗口。

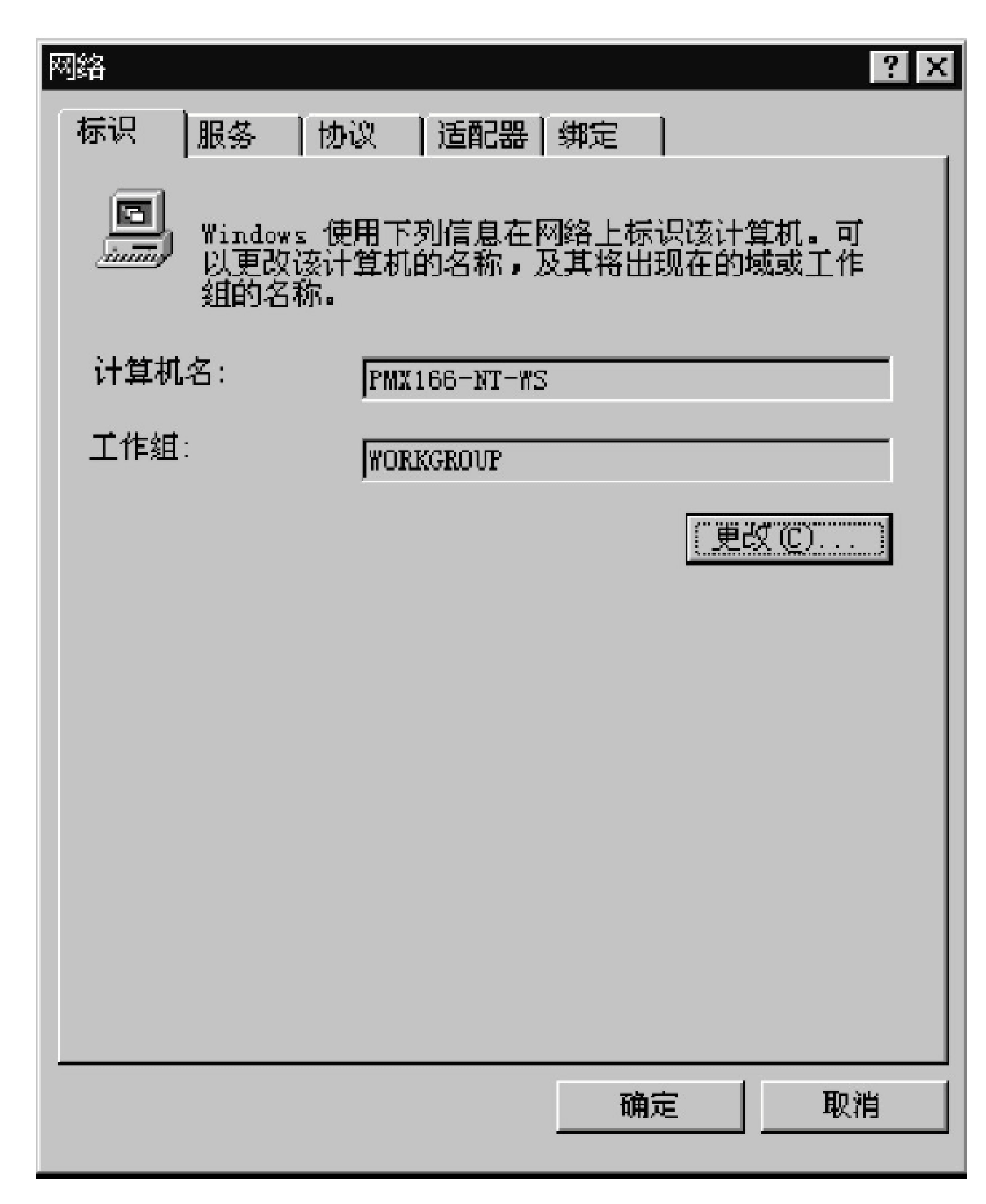


图 6-10 "控制面板"中的"网络"窗口

④ 在图 6-10 所示的窗口中,单击"更改"按钮,激活如图 6-11 所示的"标识更改"

窗口。

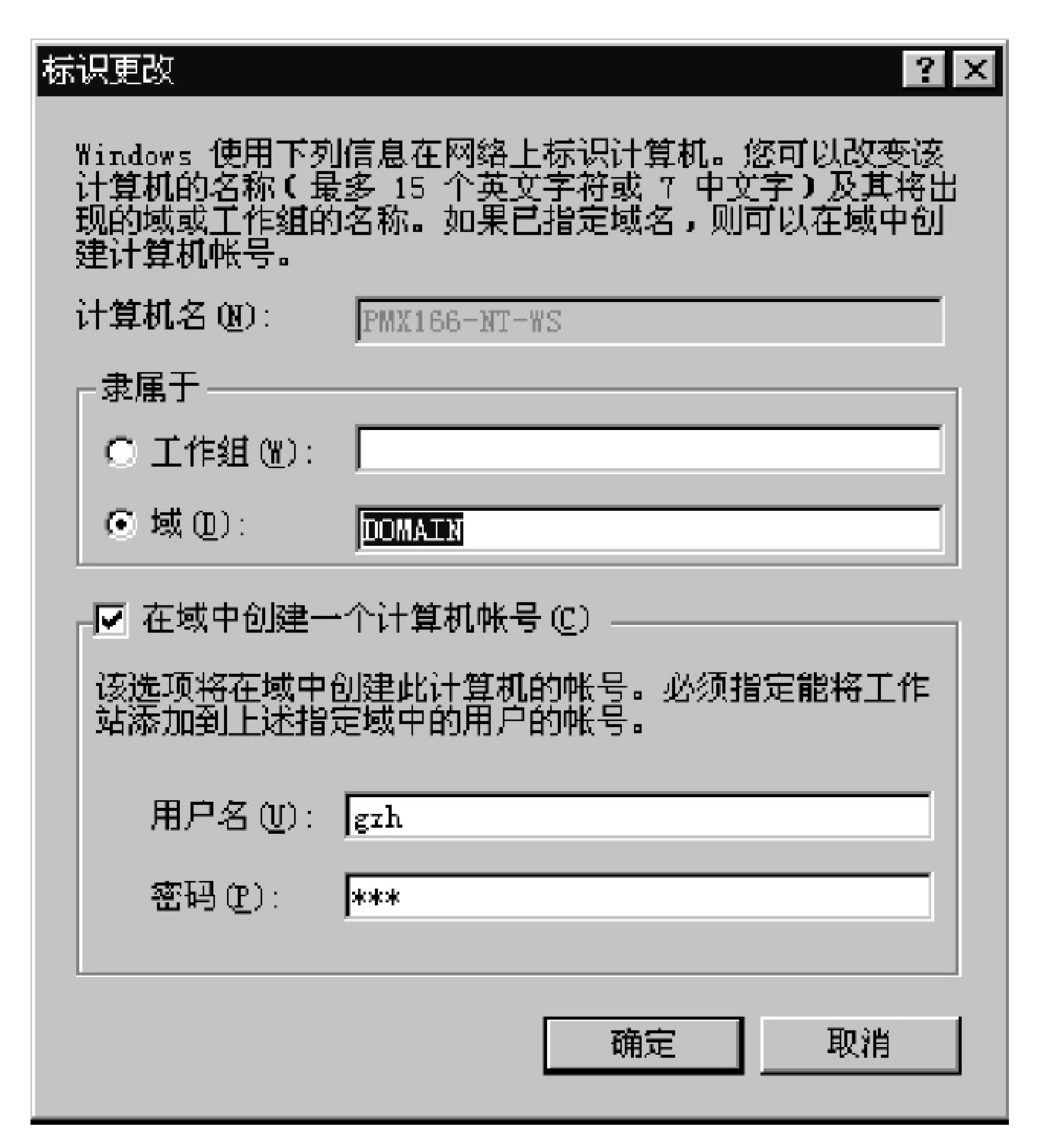


图 6-11 “标识更改”窗口

⑤ 在图 6-11 所示的“标识更改”窗口中，选中“域”单选框，并在其后的文本框中输入 NT Workstation 工作站加入的域名，例如输入 DOMAIN。

⑥ 在图 6-11 所示的“标识更改”窗口中，选中“在域中创建一个计算机账号”前的复选框，并在下面的文本框中输入计算机账号的用户名和相应的密码。注意：此计算机账号必须是在 DOMAIN 域中，具有将工作站加入“域”权利的用户账号，而不是工作站的管理员账户或其他账户。例如使用 PDC 上的域管理员账号 administrator。

⑦ 在图 6-11 所示的“标识更改”窗口中，单击“确定”按钮完成。如果成功地加入了该域，将出现欢迎窗口，提示“欢迎加入 DOMAIN”域的信息，否则提示出错信息。

⑧ 单击“关闭”按钮，出现重新启动计算机的询问窗口，在窗口中单击“是”按钮，重新启动计算机。之后，该工作站正式加入到 DOMAIN 域。

⑨ 重新启动计算机后，出现 3 栏的登录窗口。此时的目的是登录到域，因此，在登录窗口 3 栏中的最后一栏，应选择拟加入域的名称，例如 DOMAIN；前两栏则应输入在该域有效账户的用户名及相应的密码，通过域目录数据库的验证之后即可登录到该域。

(2) Windows NT 工作站加入“域”的第 2 种方法

从 NT Workstation 和 NT Server 两端进行设置，使得 NT Workstation 加入“域”的步骤如下：

① NT Server“主域控制器”端的设置。

- 以 NT Server“主域控制器”的管理员身份登录 PDC。
- 依次选择“开始”→“程序”→“管理工具”→“服务器管理器”命令选项。

• 在激活的“服务器管理器”窗口中，依次选择“计算机”→“添加到域”命令选项，激活如图 6-12 所示的窗口。



图 6-12 “添加计算机到域”窗口

• 在图 6-12 所示的窗口中，选中“Windows NT 工作站或服务器”单选钮；在“计算机名”文本框中，输入要加入域的计算机的计算机名；最后单击“添加”按钮，返回“服务器管理器”窗口，完成添加工作。

② NT Workstation 工作站端的设置。

NT Workstation 工作站端的设置步骤与(1)中的 7 个步骤类似。

3. NT Workstation 工作站登录到 NT Server“域”及资源互访

(1) NT Workstation 工作站的域用户登录 NT Server“域”

连接并设置完成之后，应首先检查网络环境，确认连接正常之后，才能使用网络资源。检查网络环境的步骤如下：

① 在 NT Server 中是否为 NT Workstation 用户建立了用于登录的用户名和密码。

② NT Workstation 计算机重新启动后，激活如图 6-9 所示的登录窗口，系统要求 NT Workstation 用户正确输入其在 NT Server 域中的合法用户名称、密码、拟登录的域名；经系统确认之后，即可进入 NT 网络系统，否则将提供出错信息。

③ NT Workstation 上的域用户注册成功后，可分别在 NT Server 与 NT Workstation 两边的计算机桌面上双击“网上邻居”图标，检查是否正确连接。在 NT Server 端双击“网上邻居”图标，注册用户计算机的图标应出现在“网上邻居”窗口内；双击其中的“整个网络”图标，出现“整个网络”窗口；选择并双击其中的 Domain 图标，出现所在域 Domain 的窗口；选择并双击“域”中的某计算机图标，如 Nt-s-586100，可以打开该计算机的窗口。域中的各合法用户都可以选择和使用该计算机上开放的所有共享资源。

④ 如果“网上邻居”中不能出现网络上其他用户的图标，则应检查网卡和协议等项的设置。

(2) 在安装了 NT Server 和 NT Workstation 的各种计算机上开放和使用共享资源

在安装了 NT Server 和 NT Workstation 的各种计算机上开放和使用域中的共享资源，进行网络互联的方法与 Windows 95/98/Me 类似，请参考 6.7.3 中的步骤依次进行即可。

6.7.3 Windows 95/98 工作站与 NT Server 的“域”方式互联

Windows 95/98 工作站与 NT Server 的连接设置与前面所述的 NT Workstation 类似，本小节仅将在 Windows 95/98 上有关网络软件的安装和设置步骤简述如下：

1. Windows 95/98 为登录 NT Server “域”做的设置

(1) 检查连网硬件和操作系统

检查所使用的网络硬件是否已经连接好，Windows 操作系统是否已经安装，一切就绪后，下面的工作是如何在 Windows 95/98/Me 下配置网卡、协议等与网络相关的信息。

(2) 在 Windows 95/98 下添加并设置网卡

对于 ISA 网卡，在 DOS 下使用网卡自带的驱动程序设置和检测之后，还要到各种工作站的操作系统(例如 Windows 95/98/Me)内进行网卡的添加和设置。这些工作站设置的参数值，应以 DOS 下设置的参数为准。而对于 PCI 网卡一般只需在 Windows 95/98/Me 下进行安装。

在图 6-14 所示的窗口中，单击“资源”选项卡，从中选择可以配置的“I/O 地址范围”等信息。设定后，单击“确定”按钮，重新启动计算机，使设置生效。至此，网卡的设置过程结束。

(3) 设置用户的常规信息

(4) 选择用户操作类型

(5) 选择由 Windows 95/98/Me 登录到 NT Server 的“域”

(6) 选择和设置网络通信协议

至此，在 NT Server 中的 TCP/IP 协议已设置完毕，如果有问题可依次检查网卡、网卡驱动程序、网络协议等各项内容。

2. NT Server 端为 Windows 95/98/Me 工作站登录到 “域”所做的设置

① 在 NT Server 端的“域用户管理器”中，分别为每个从 Windows 95/98/Me 工作站登录域的用户建立用户账号，包括用于登录验证的用户名和密码等信息。

② 为上述用户账号设置访问权限，以便按规定的权限访问共享资源。例如：域的系统管理员在 NT Server 上的“域用户管理器”上，建立新用户账号“zdh01”、“zdh02”等，并将它们加入到“Domain”域，还要设置好访问权限。

3. Windows 95/98/Me 工作站登录 NT Server“域”及资源互访

(1) Windows 95/98/Me 计算机的域用户“登录”NT Server“域”

① Windows 95/98/Me 计算机重新启动后，激活如图 6-13 所示的登录窗口，系统要求 Windows 95/98/Me 用户正确输入其在 NT Server 域中的合法用户名称、密码，并在注册窗口的第 3 栏，输入要登录的域名；经 NT 系统中的 PDC 或 BDC 验证确认之后，即可进入 NT 网络系统，否则会提供出错信息。

② 在 Windows 95/98/Me 注册成功后，可分别在 NT 服务器和 Windows 95/98/Me 两边的计算机桌面上双击“网上邻居”图标，检查是否正确连接，并选择、使用网络中计算机上的所有允许访问的共享资源。

(2) Windows 95/98/Me/NT 计算机上开放和使用共享资源

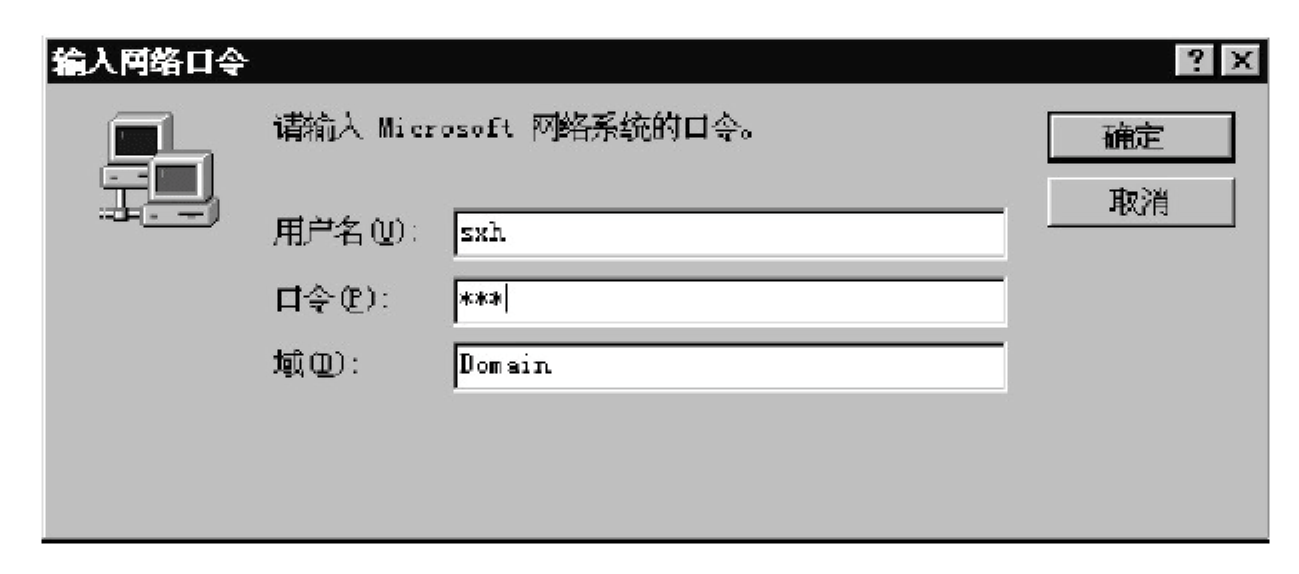


图 6-13　Windows98 启动后的”登录”窗口

无论是在 Windows 95/98/Me 计算机上，还是在 NT 计算机上，开放和使用共享资源的方法都十分类似。当开放资源时，第 1 步，在开放资源的计算机的“资源管理器”中，选择拟开放的共享资源。第 2 步，设置共享资源的访问权限。

在 Windows 95/98/Me 计算机上的“资源管理器”中开放共享资源的步骤如下：

① 在 Windows 95/98/Me 计算机上，依次选择“开始”→“设置”→“控制面板”命令选项，在打开的窗口中，双击“网络”图标，激活“网络”窗口。

② 在网络窗口的“配置”选项卡中，单击“文件和打印共享”按钮，激活如图 6-14 所示的窗口，选中其中的两个复选框。

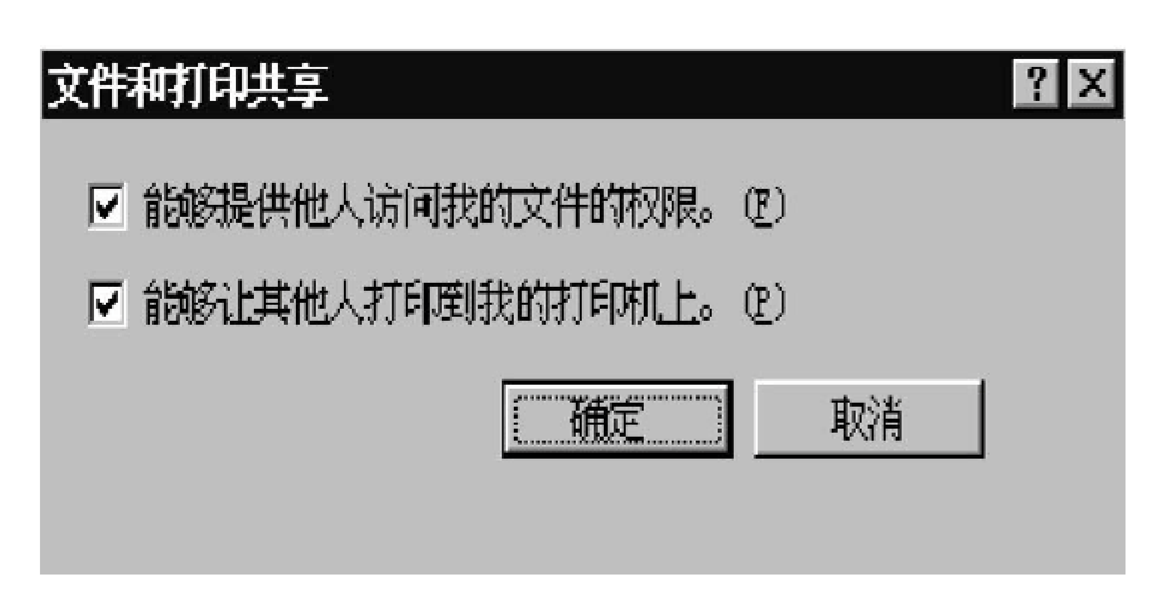


图 6-14　“文件和打印共享”窗口

③ 在 Windows 95/98/Me 桌面上选择“我的电脑”图标，单击鼠标右键，激活如图 6-15 所示的快捷菜单。在快捷菜单中，单击“资源管理器”命令，打开图 6-16 所示的窗口。



图 6-15　右击桌面的“我的电脑”图标显示快捷菜单

④ 在图 6-16 所示的“资源管理器窗口”中选择允许他人访问的资源，例如：“E:\瑞星

杀毒软件”，单击鼠标右键，激活该选项处的快捷菜单。

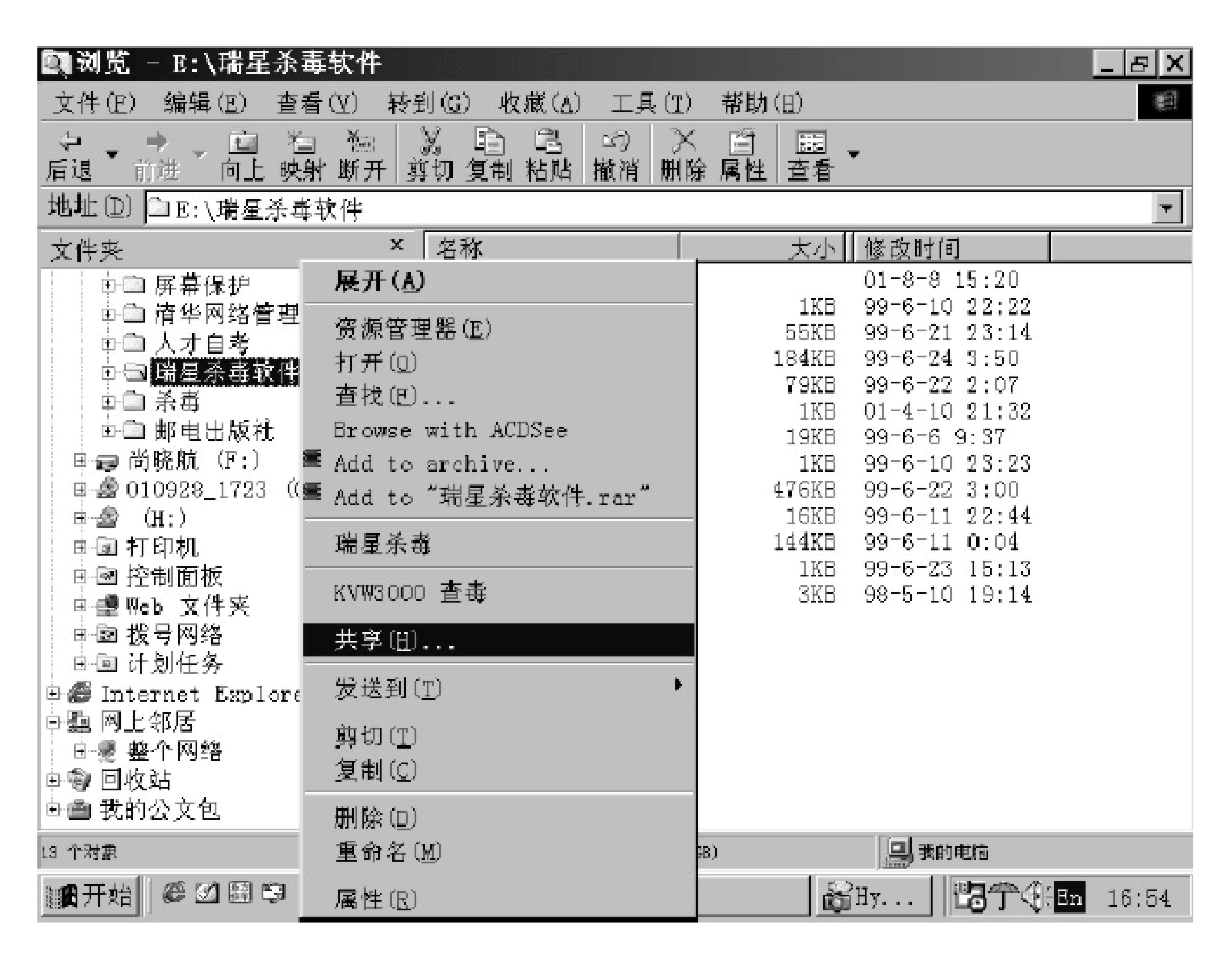


图 6-16　Windows 95/98/Me 的“资源管理器”窗口及右键激活的快捷菜单

⑤ 在弹出的快捷菜单中，单击“共享”选项，激活如图 6-17 所示的窗口。



图 6-17　Windows 98 中的“瑞星杀毒软件 属性”窗口

⑥ 在图 6-17 所示的窗口中，单击“共享”选项卡，选中“共享为”，根据情况设置该共享资源的被访问权限，例如“只读”。单击“确定”按钮，返回“资源管理器”，如果所设置的资源下面出现一只“共享小手”，则表示共享设置成功。

说明：在 Windows NT 计算机上开放共享资源的设置方法与 Windows 95/98/Me 类似，请参考上述步骤依次进行。

在 Windows95/98/Me 计算机上使用网络共享资源的方法也有以下两种：

第 1 种：Windows 95/98/Me 计算机桌面上的“网上邻居”中直接浏览、复制和使用已共享的资源。

第 2 种：用“映射网络驱动器”的方法使用域中各个计算机上开放的共享资源。

前一种的方法比较简单，不作详细介绍，后一种方法的操作步骤如下所述：

① 在 Windows 桌面上选择“我的电脑”图标，单击鼠标右键，激活快捷菜单。

② 在快捷菜单中，单击其中的“映射网络驱动器”选项。

③ 在激活的图 6-25 所示的“映射网络驱动器”窗口中的“驱动器”文本框中，选择网络驱动器的代号，例如 G；在“路径”文本框中，输入 NT 端的共享资源的路径和名称，其语法为：\\资源所在计算机的名称\资源的共享名例如\\Nt-s-586100\Nt-C，其中“Nt-s-586100”为资源所在计算机的名称；Nt-C 为该计算机上的共享资源名称，此命令的含义是将网络上名称为“Nt-s-586100”计算机上的共享资源 Nt-C 映射为本计算机上的 G 驱动器。

④ 若用户打算每次登录时，都让 Windows 95/98/Me 计算机连接到这个共享资源，则可在图 6-18 中，选中“登录时重连接”，设置好之后，单击“确定”按钮，返回资源管理器窗口。



图 6-18 “映射网络驱动器”窗口

⑤ 连接成功之后，驱动器 G 就代表 NT 网络上名为“Nt-s-586100”的计算机上的共享资源 Nt-C，使用映射网络驱动器 G 的方法与使用局部硬盘一样。在资源管理器中，双击映射的网络驱动器 G，即可展开异地计算机上共享资源 Nt-C 中的内容。

（3）断开网络驱动器

无论是在 NT 网络服务器上，还是在 Windows 95/98/Me 上，断开“网络驱动器”连接的方式均有以下两种：

① 在 Windows 的“资源管理器”窗口中，选中需要断开的网络驱动器，例如：选中网络驱动器 G，单击鼠标右键，激活快捷菜单条，从中选择“断开(D)”选项，完成选中网络驱动器的断开过程。

② 在 Windows 95/98/Me“资源管理器”中，选择“工具”→“断开网络驱动器”命令选项，在激活的窗口中选择需要断开的网络驱动器，例如，选择网络驱动器 G，单击“确定”按钮，也可完成选中网络驱动器的断开过程。

6.7.4　各种 DOS 工作站与 NT Server 的“域”方式互联

当工作站配置较低，或者需要迅速连入 Windows NT 服务器，以便使用其中的共享资源时，可以采用以下 3 种连接方式：

① MS network client 方式。

② LAN manages 方式。

③ DOS 启动盘方式。

其中常用的有以下两种：

- DOS 工作站与 NT Server“域”方式互联；
- DOS 无盘工作站与 NT Server“域”方式互联。

无论哪种方式，互联时的主要步骤均与上述的类似，即分为“服务器端”、“客户工作站”端和“资源共享”几部分。如果互联时出现故障，应当先查硬件的连通性，再按上述几部分进行检查，受篇幅所限本章不再多作介绍。

习题

(1) 如何安装、连接、设置和诊断网络适配器(网卡)? 需要注意些什么?

(2) 安装 NT 的媒介和方式共有几种? 各适用在什么场合下?

(3) 安装 NT 时对硬件的要求有哪些?

(4) FAT 与 NTFS 文件系统有什么区别? 各适应什么场合?

(5) NT 网络有几种模型? 应如何选择?

(6) 什么是“域”的网络组织方式? 建立“域”有什么好处? 适用在什么场合?

(7) 什么是“工作组”的网络组织方式? 这种方式的特点是什么? 适用在什么场合?

(8) “工作组”和“域”的组织方式有何不同?

(9) 请说明选择 NTFS 和选择 FAT 文件系统格式的理由。

(10) 解释、说明一个硬盘在如何分区的情况下，可以同时使用 FAT 和 NTFS 文件系统格式。

(11) 在安装 Windows NT 软件时主要的安装方式有几种? 各有什么特点?

(12) 典型式(即快速)安装与定制安装之间有何区别?

(13) 在安装过程中，用户希望能手动配置安装一些网络组件，应选择何种安装方式?

(14) 在安装过程中，当你发现，有 1 个硬件不在 NT Server 提供的硬件设备 HCL 表中时，应该怎么办?

(15) 如何卸载 NT Server 或者 NT Workstation? 分别写出在 FAT 和在 NTFS 文件格式的分区上卸载 Windows NT 的主要步骤。

(16) 安装 NT Server 软件的服务器分为几种类型? 各有什么作用? 这几种类型的 NT 服务器可否相互转换? 转换的条件是什么?

(17) 什么是目录数据库? 它根据网络的组织方式的不同分为几种? 区别如何?

(18) 目录服务的目标是什么？NT 网络是如何实现这个目标的？

(19)“域”的模式下如何实现资源的互相访问？试说明“域”和“工作组”模式下使用共享资源的区别。

实训题目

1. 选择、创建和删除 NTFS 系统分区。

2. 在选定的计算机上安装 NT Server 或 NT Workstation 系统。

3. 安装 Windows 98、NT Server 和 NT Workstation 多引导系统。

4. 制作 3 张系统引导“安装磁盘组”和“紧急修复磁盘”，使用它修复 1 台类似计算机的 NT 系统。

5. C/S 模式网络实验：NT Server 与 NT Workstation 工作站“域”方式互联操作与资源互访。

6. C/S 模式网络实验：NT Server 与 Windows 95/98/Me 工作站“域”方式互联操作与资源互访。

7. 对等网实验(按本章介绍的连接要点选做)：两台或多台 NT Workstation 工作站之间“工作组”方式互联操作与资源互访。

8. 对等网实验(按本章介绍的连接要点选做)：Windows 95/98/Me 工作站与 NT Workstation 工作站之间“工作组”方式互联操作与资源互访。



网络中的 TCP/IP 管理

协议是网络通信的语言，因此，可以说协议是网络的本质，而有关通信协议的配置和管理也是网络管理员的一项重要工作。本章主要介绍 NT 网络中，有关 TCP/IP 协议的配置和管理技术。

主要内容：

- 常用协议的选择和比较；
- TCP/IP 四层参考模型；
- Windows NT 中的 TCP/IP；
- TCP/IP 协议的 3 个基本参数；
- TCP/IP 的安装与测试；
- TCP/IP 协议中 IP 地址的管理；
- 静态 IP 地址和动态 IP 地址；
- 子网划分；
- 动态 IP 地址的管理；
- DHCP 服务器和客户机的安装、设置与管理。

7.1 TCP/IP 协议基础

随着 Internet 的飞速发展，各种使用 Internet 技术的网络和软件广为流行，因此，越来越多的公司选择 TCP/IP 协议作为网络的主要协议，TCP/IP 协议已经成为事实上的工业标准，并且得到了所有主流操作系统和众多厂商的广泛支持。然而，对于局域网来说，TCP/IP 协议并不是最简单、最快的网络协议。

TCP/IP(transmission control protocol/Internet protocol)，中文名称为"传输控制协议/网际协议"。TCP/IP 是一个 32 位的、可路由的工业标准的协议集。它是目前使用最为广泛的通信协议。TCP/IP 模型中又包含了许多通信标准，以便规范网络中计算机的通信和连接。由于在 Intranet 中广泛采用了 Internet 技术，因此，网络管理员对于 Internet 中最重要的 TCP/IP 通信协议，应该很好地理解；并应熟练掌握该协议的配置、

检测和管理技术。

7.1.1 TCP/IP 的 4 层参考模型

1. 网络接口层

网络接口层为 TCP/IP 模型的底层(也被称为链路层,或主机-网络层)。它与 OSI 模型的下两层相对应,即物理层与数据链路层。TCP/IP 标准并未定义具体的网络接口层协议,这样提高了灵活性,可以适应各种网络类型,如 LAN、MAN 和 WAN。因此,TCP/IP 可以运行在任何网络之上。

2. 网际层(IP)

TCP/IP 模型的网际层,也称 IP 层、网间网络层。它与 OSI 模型的网络层相对应。网际层负责管理不同网络设备之间的数据交换。IP 层包含以下几个主要的协议:

① IP(Internet protocol,网际协议) IP 使用 IP 地址确定收发端,提供端到端的"数据报"传递。IP 协议还规定了计算机在 Internet 上通信时所必须遵守的一些基本规则,以确保路由的正确选择和报文的正确传输。

② ICMP(Internet control message protocol,网际控制报文协议) 用于处理路由,协助 IP 层实现报文传送的控制机制。如,传送控制信息,提供错误信息报告。

③ ARP(address resolution protocol,地址解析协议) 用于完成 IP(Internet)地址向物理地址的转换,即把 IP 地址映射到远程局域网的硬件物理地址。

④ RARP(reverse address resolution protocol,逆向地址解析协议) 用于完成物理地址向 IP 地址的转换。

3. 传输层(TCP)

TCP/IP 模型的传输层在 IP 层之上,与 OSI 模型中的传输层的功能相对应。传输层提供端到端的通信服务,即网络节点之间应用程序的通信服务,并确保所有传送到某个系统的数据能够正确无误地到达该系统。传输层包含的两个主要协议都是建立在 IP 协议的基础上的,其功能如下所述:

① TCP(传输控制协议) 提供面向连接的可靠数据传输服务。它通过认证方式、重传机制等确保数据的可靠传送。它适合于每个分组仅含少量字符的交互式终端的应用,也适合大数据量的文件传输。

② UDP(用户数据报协议) 采用无连接的数据报传送方式,提供不可靠的数据传送。UDP 方式与 TCP 相比,更加简单,数据传输速率也较高。当通信网络可靠性较高时,UDP 方式具有更高的优越性。

4. 应用层

TCP/IP 模型的应用层与 OSI 模型的上 3 层对应。

(1) 应用层的功能

应用层向用户提供调用和访问网络中各种应用程序的接口;并向用户提供各种标准的应用程序及相应的协议。用户还可以根据需要建立自己的应用程序。

(2) 应用层的协议

应用层的协议有很多种,主要包括以下几类:

① 依赖于面向连接的 TCP 协议的应用层协议有以下几种：

- Telnet，虚拟终端服务，使用默认端口 23，它允许一台主机上的用户登录到另一台远程主机，并在该主机上进行工作，用户所在主机仿佛是远程主机上的一个终端。
- SMTP，电子邮件服务，使用默认端口 25，以电子数据的方式，使用户可以快捷、方便地传送信息。
- FTP，文件传输协议，使用默认端口 21，为文件的传输提供了途径。它允许将数据从一台主机上传输到另一台主机上，也可以从 FTP 服务器上下载文件，或者向 FTP 服务器上载文件。
- NetBIOS 对话服务。

② 依赖于无连接的 UDP 协议的应用层协议，及其以 socket 程序为基础的应用程序。

- SNMP，简单网络管理协议。
- TFTP，单纯文件传输协议。
- DOMAIN，域名服务程序。
- NetBIOS-NS，NetBIOS 名字服务程序。
- RPC，远程过程调用协议。

③ 既依赖于 TCP 协议也依赖于 UDP 协议的应用层协议有以下几种：

- CMOT，通用管理信息协议。
- DNS，域名系统服务协议，使用默认端口 53。

④ 非标准化协议。即属于用户自己开发的专用应用程序，它们是建立在 TCP/IP 协议簇基础之上，但无法标准化的程序。例如，Windows sockets API 为使用 TCP 和 UDP 的软件提供 Microsoft Windows 下的标准应用程序接口，在 Windows sockets API 上的应用软件可以在 TCP/IP 的许多版本上运行。

TCP/IP 协议作为高层协议来说，是世界上应用最广的异种网互联的标准协议，利用它，异种机型和使用不同操作系统的计算机网络系统就可以方便地构成单一协议的互联网络（TCP/IP 网络）。

7.1.2 Windows NT 中的 TCP/IP

Windows NT 中的 TCP/IP 协议使得企事业单位的计算机网络化更为方便，它有如下一些优越性：

- TCP/IP 是一个工业标准的、可路由的网络协议，它能够提供不同类型环境下的通讯连接，现在的绝大多数操作系统都支持 TCP/IP；
- TCP/IP 提供了异种网络系统之间连接技术，使用 TCP/IP 协议，能够在 Microsoft、IBM SNA Network、UNIX、TCP/IP Host、Netware 之间建立连接；
- TCP/IP 提供了以 NT 计算机访问世界范围内 Internet 及其资源的能力。

1. Windows NT 提供的实用程序

TCP/IP 实用程序与 TCP/IP 协议共同提供了访问异种主机和 TCP/IP 因特网的能力。Windows NT Server 4.0 提供了许多 TCP/IP 实用程序，参见表 7-1。

表 7-1　Windows NT Server 中的 TCP/IP 实用程序及其功能表

TCP/IP 协议（实用程序）	协议全名	可选参数	程序功能
PPP	点对点协议		用于连续的 IP 通信
FTP	文件传输协议	-?	在 Windows NT 计算机与其他运行 FTP 服务器的 TCP/IP 主机之间用 ftp 可以进行双向文件传输
Telnet	终端仿真协议		提供远程终端仿真
ICMP	Internet 控制报文协议		用于故障检测，如，ping 命令可以验证 TCP/IP 协议的配置和网络连通状况
UDP	用户数据报协议		无连接数据传输
TFTP	小文件传送协议	-i，	在 Windows NT 计算机与其他运行 TFTP 服务器的 TCP/IP 主机之间用 tftp 可以进行双向文件传输
tracert	跟踪命令	-d -h…	显示在网络上的传输路径
route	路由表管理命令	-f print MASK…	用于管理本地的 TCP/IP 路由表
nbtstart		-r -R	用来显示 TCP/IP 上的 NetBIOS 状态
ipconfig	IP 配置协议	/all	该诊断命令显示当前 TCP/IP 网络中的所有配置信息
ping	基本 TCP/IP 诊断程序	-? -t -a -f…	该诊断命令通过向网络上发送 ICMP 包来校验网络的连通性
Hostname			显示当前计算机（主机）的名称

有关各种命令或者其他命令的详细使用方法，在“我的电脑”中，选择下拉菜单中的“帮助主题”选项后，键入命令就可以得到相关的帮助信息。

2. Windows NT Server 提供的 TCP/IP 服务

Windows NT Server 4.0 中的 TCP/IP 除了具有以上的优越性之外，它还支持以下几个高级服务：

① DHCP(dynamic host configuration protocol)，动态主机配置协议；

② WINS (windows Internet name service)，网际命名服务；

③ DNS(domain name system)，域命名系统；

④ TCP/IP 打印服务，允许从 UNIX 环境访问打印机。

7.1.3　TCP/IP 协议的 3 个基本参数

本小节首先介绍有关地址的几个基本概念，然后讲解在安装和配置 TCP/IP 协议时需要使用的 IP 地址、子网掩码和默认网关这 3 个基本参数。

1. 网络地址有关的概念

(1) 网络地址的意义与组成

网络地址用来标识网络中的各种对象，因此又叫做“标识符”。标识符有 3 类，即名字(name)、地址(address)和路径(route)，它们分别告诉人们，对象是什么、去何处和怎样去寻找对象。

(2) 物理地址和 IP 地址

① 物理地址。

在任何一个物理网络中，网络中的任何两台主机之间通信时，都必须获得对方的一个可以识别的地址，才能使信息在其中进行交换，这个地址就是物理地址（physical address）。

② IP 地址。

IP 协议提供了一种全网统一的地址格式。在统一方式的管理下进行地址的分配，从而保证了一个地址对应一台主机（包括路由器或网关）。这个地址就是 Internet 上使用的逻辑地址，简称为“IP 地址”。IP 地址与硬件无关，不管主机连接到什么样的网络上，都可以使用 IP 地址进行惟一标识。

（3）地址解析

Internet 利用 IP 地址统一了各自为政的物理地址，然而，这种统一表现在自 IP 层以上使用了统一格式的 IP 地址，而将物理地址隐藏了起来。实际上，各种物理地址并未改动，在物理网络的内部仍然使用各自原来的物理地址。由于物理网络的多样性，决定了网络物理地址的五花八门。因此，在使用 Internet 技术的网络中，就必然存在着两种地址，即 IP 地址和各种物理网络的物理地址。若想把这两种地址统一起来，就必须建立两者之间的映射关系。这种地址之间的映射就称为“地址解析（resolution）”，它包括以下两方面的内容：

① 从 IP 地址到物理地址的映射。TCP/IP 协议中完成此功能的协议为正向地址解析协议 ARP。

② 从物理地址到 IP 地址的映射。TCP/IP 协议中完成此功能的协议为逆向地址解析协议 RARP。

2. IP 地址及其规定

（1）编址

Internet 是通过 TCP/IP 协议和网关（或 IP 路由器）等设备将各种物理网络互联而成的虚拟网络。通俗地说，在 Internet 中，每一台计算机（主机）都有一个惟一的 IP 地址。这个 IP 地址在网络中的作用就像住户的地址，根据这个 IP 地址，可以找到这台计算机所在网络的编号；以及该计算机在该网络上的主机编号。IP 地址结构如图 7-1 所示。即每一个 IP 地址都由两部分组成，网络地址（即网络 ID 或网络编号）和主机地址（即主机 ID 或主机编号）。

网络地址	主机地址

图 7-1　TCP/IP 网络中 IP 地址的结构

由 TCP/IP 协议规定的 IP 地址由 32 位二进制的比特位组成，每个 IP 地址由 4 个部分对应的十进制数字组成，每部分用“.”分隔，例如 202.4.192.111。在使用 TCP/IP 协议的网络中的每一台 TCP/IP 主机都必须分配一个惟一的 32 位地址。

（2）网络地址

网络地址也称网络编号、网络 ID 或网络标识。网络地址用于辨认网络，同一网络上

的所有 TCP/IP 主机的网络 ID 都相同。

(3) 主机地址

主机地址也称主机 ID、主机编号或主机标识,它用于辨认网络中的主机。

3. IP 地址的划分

每台运行 TCP/IP 协议主机的 IP 地址必须惟一,否则就会发生 IP 地址的冲突,导致计算机之间不能很好通讯。

(1) IP 地址的类别

根据网络的大小,Internet 委员会定义了 5 种标准的 IP 地址类型,以适应不同规模的网络。在局域网中仍沿用这个分类方法,但是 Microsoft NT 只支持其中的 3 类,即表 7-2、表 7-3 和表 7-4 中所描述的 A、B 和 C 类网络。

① A 类地址:A 类地址分配给拥有大量主机的网络。A 类地址的“W”字段内高端的第一位总为“0”,接下来的 7 位表示网络 ID。剩余的 24 位(即 X、Y、Z 字段)表示主机编号。它允许有 126 个网络和大约 1 700 万个主机。

② B 类地址:B 类地址一般分配给中等规模的网络。B 类地址的“W”字段内的高端的前两位为“10”,接下来的 14 位表示网络 ID。其余的 16 位(即 Y、Z 字段)表示主机编号。它允许有 16 384 个网络和大约 65 000 个主机。

③ C 类地址:C 类地址一般分配给小规模的网络。C 类地址的“W”字段内的高端的前三位为“110”,接下来的 21 位表示网络地址(ID)。其余的 8 位(即 Z 字段)表示主机编号。它允许约有 200 万个网络,每个网络有 254 个主机。IP 地址的类型定义了网络地址(ID)使用哪些位,主机编号(ID)使用哪些位,同时也定义了每类网络中包含的网络数目和每类网络中可能包含的主机数目。表 7-2 表明了各类标准 IP 地址的定义,以及网络地址和主机编号字段的取值范围。

表 7-2 网络类别、网络地址和主机编号字段的取值范围

网络类别	IP 地址	网络地址	主机编号	网络地址(W)的取值范围	主机个数
A	W.X.Y.Z	W	X.Y.Z	1~126	1 700 万左右
B	W.X.Y.Z	W.X	Y.Z	128~191	65 000
C	W.X.Y.Z	W.X.Y	Z	192~223	254

表 7-3 归纳了 A、B、C 3 类网络的 IP 地址取值范围。在 Internet 中,IP 地址的使用和分配由专门机构管理,但局域网中却不必受上述规定的约束。

表 7-3 A、B、C 3 类网络的特性参数取值范围

网络类别	网络地址(W)的取值范围	网络个数	主机个数
A	1.X.Y.Z ~126.X.Y.Z	126	大约 1 700 万个
B	128.X.Y.Z ~191.X.Y.Z	16 384	65 000
C	192.X.Y.Z ~223.X.Y.Z	大约 200 万个	254

(2) IP 地址中网络地址的使用规则

无论在 Internet 上还是在局域网上,分配网络地址(即网络 ID)时,常用的 A、B 和 C

类网络的取值范围如表 7-4 所示，配置和使用 IP 地址时，应遵循以下规则：

① 网络地址必须是惟一的。

② 网络地址不能以 127 开头。因为，127 保留给诊断用的回送函数使用。

③ 网络地址的各位不能全为“1”(即十进制的 255)。255 作为广播地址。

④ 网络地址的各位不能全为“0”。0 表示局部网络。

表 7-4　A、B、C 网络地址和主机编号的取值范围

网络类别	网络地址始值	网络地址终值	主机编号始值	主机编号终值
A	001.X.Y.Z	126.X.Y.Z	W.0.0.1	W.255.255.254
B	128.0.Y.Z	191.255.Y.Z	W.X.0.1	W.X.255.254
C	192.0.0.Z	223.255.255.Z	W.X.Y.1	W.X.Y.254

(3) IP 地址中主机编号的使用规则

① IP 地址中主机编号的各位不能全为“0”。

② IP 地址中主机编号的各位不能全为“1”。

③ “127.0.0.1”代表本地主机的 IP 地址，因此，该地址不能分配给网络上的任何计算机使用。

(4) IP 地址的分配和使用的基本原则小结

在 Internet 中 IP 地址的分配由指定的机构进行。在局域网内 IP 地址的分配可以不受限制。由上面的分析可知，无论在 Internet 中，还是在局域网中，为了区分网络和主机，IP 地址的分配应遵循如下原则：

① 同一个网络内的所有的主机必须分配相同的网络地址，而同一个网络内的所有主机必须分配不同的主机编号。例如下例中的 A 和 B 主机。

② 不同网络内的主机必须分配不相同的网络地址，但是可以分配相同的主机编号，例如下例中的 A 和 X 主机。

③ 因为仅使用 IP 地址无法区分网络地址和主机编号，因此，必须结合子网掩码一起使用。例如：下例中的 132.112.000.001，在网络中，可以认为网络标识号为“132”，也可以认为是“132.112”。

4. 子网掩码(subnet masks)

(1) 子网

人们常常把一个较大的网络分成多个较小的网络，每个小网络使用不同的网络编号，这样的小网络被称为“子网”。通过路由器可以将多个子网连接起来。

(2) 子网掩码的功能与使用

为什么需要网络编号？在两台计算机之间进行通讯时，一般用户可能认为只要知道了对方的 IP 地址就可以进行通信了，但是，实际上在这两台计算机之间存在的通信路径可能有很多条。因此通信时，两边的计算机首先需要判断彼此是否在同一个网络上，如果是在同一网络上，就直接进行通信；否则就转发到本网的出口，由该出口负责处理并发送到目的网络上。

子网掩码与 IP 地址一样也是一个 32 位的二进制比特值，用它可以屏蔽一部分 IP 地

址，以便区分出 IP 地址中的网络编号和主机编号。当使用 TCP/IP 通信时，子网掩码主要用来确定目的主机是位于本地子网还是远程网，它的两大功能如下：

① 用于区分 IP 地址中的网络地址和主机编号。

不同类型的网络使用的子网掩码是不同的，表 7-5 给出了 Windows NT 中各类网络所默认的子网掩码。

表 7-5 各类网络默认的子网掩码

网络类别	子网掩码（以二进制位表示）	子网掩码（以十进制位表示）
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

实例 对图 7-2 所示的系统进行通信分析。

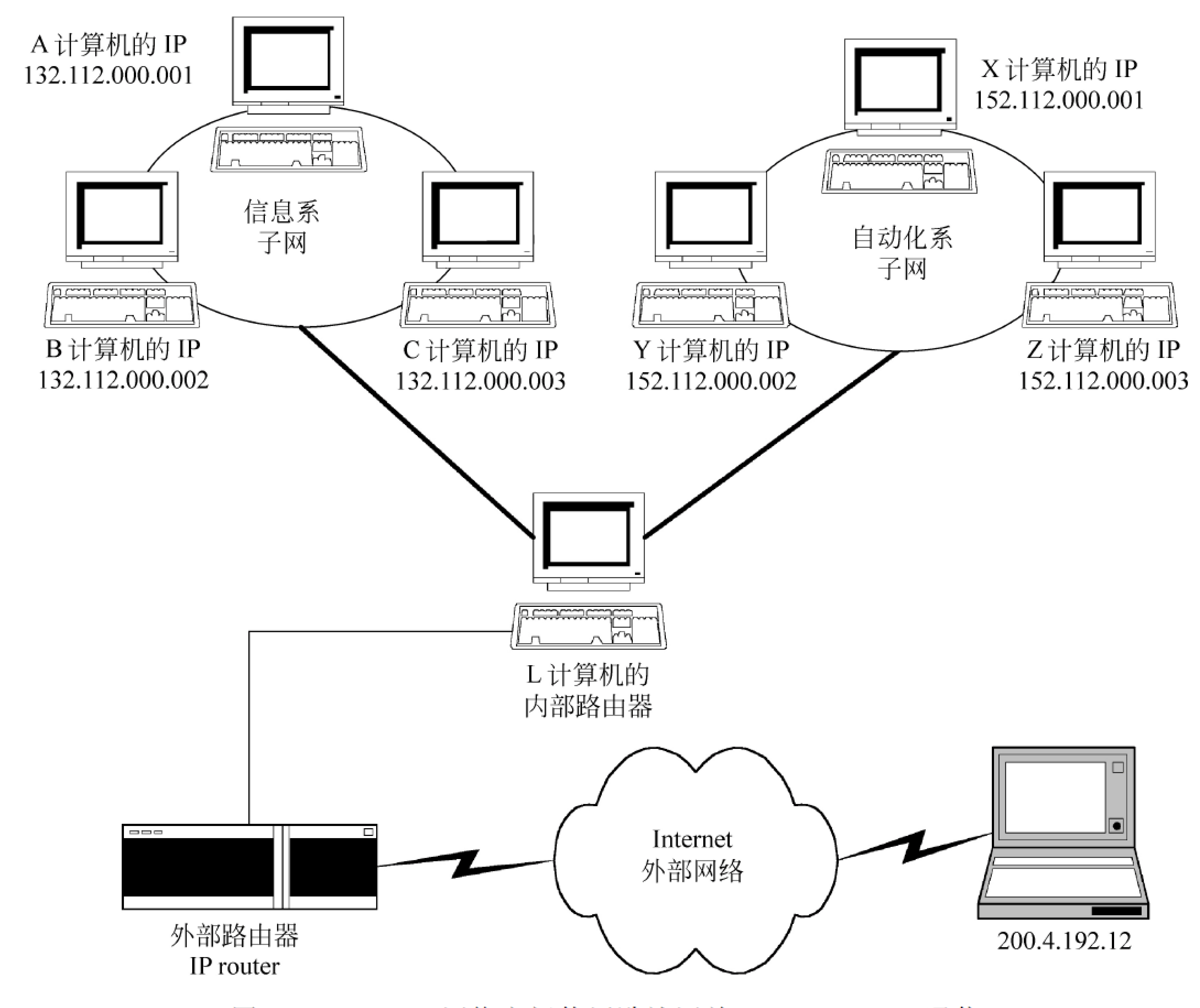


图 7-2 TCP/IP 网络之间使用默认网关（IP ROUTER）通信

解：

ⓐ 用 IP 地址的第一段数值 W 判断网络类型。在本例中，计算机 A，B，X 的 IP 地址中 W 的值分别等于 132、132 和 152。因此，由表 7-3 可知这三个计算机所在的网络均为 B 类网。

ⓑ 通过子网掩码求网络地址的步骤如下，结果见表 7-6。

- 将 IP 地址转化为 32 位二进制位。
- 将子网掩码也转化为 32 位二进制位。
- 将 3 个二进制表示的 IP 地址分别和二进制表示的子网掩码，按位进行“逻辑与(AND)”操作。按此方法依次求得数值之后，再按原有的 4 段分别转换为十进制数。

说明：其中子网掩码为“1”的各位所对应的 IP 地址中的各位，即为网络地址，也称网络标识或网络 ID。运算结果见表 7-6。

ⓒ 网络内的主机编号(HOST ID，即主机标识)。

在 IP 地址中扣除网络地址外的其余部分就是主机编号部分。由于是默认的 B 类网络，其 IP 地址在扣除了网络地址后，剩余的 2 个字段表示该主机在其子网内的编号部分。经简化得到 3 个主机编号分别为：1、2 和 1，参见表 7-6。

表 7-6　IP 地址划分实例分析计算结果

网络类别	计算机名称	“逻辑与”的结果	网络地址	计算机编号部分	主机编号
B	A	132.112.0.0	132.112	000.001	1
B	B	132.112.0.0	132.112	000.002	2
B	X	152.112.0.0	152.112	000.001	1

ⓓ 用“网络地址”即网络编号判断这几个网络是否在同一个子网上。

由于，A 和 B 主机的网络地址均为“132.112”，因此这两台主机在同一子网上；而 X 主机的网络地址为“152.112”，所以该主机在另一个子网上。如果 A 主机与 B 主机进行通信，可以直接进行通信。而如果 A 主机与 X 主机进行通信，则需要通过网络中 L 主机所代表的内部路由器(或内部网关)。如果这些子网中的主机需要与外部网络进行通信，则还需要通过外部路由器。

② 划分子网。

子网掩码的另一个重要功能是用来划分子网，即将一个网络分为多个子网。在实际应用中，经常遇到网络地址不够的问题。例如，仅申请到一个可以在 Internet 上使用的 IP 地址，而需要划分的内部子网数目为多个。这种情况下，就需要把某种类型的网络划分成多个子网。其思路就是将“原来”(申请的)主机编号部分的一些二进制位贡献出来，用于内部网络的编号。由于从 Internet 到此网络的路径都是一样的(即申请到的 IP 地址的网络地址部分不变)，因此，外界到此网络中各子网的路由都是一样的。这种情况下，外部路由将所有子网看成一个网络，而内部的路由器可以区分出不同子网。下面通过一个实例来说明划分子网的步骤。

③ 划分子网的实例和规则。

实例：已申请到的 C 类 IP 地址为 202.4.192.x，即其外部路由的网络地址为“202.4.192”，现在需要划分 5 个内部子网，每个子网的主机个数不少于 20 个。

解：划分子网的步骤如下所述：

ⓐ 求取主机编号部分转化为子网掩码部分的位数 m。

先确定所要划分的子网数目的最大值 N_{max} 和允许的最大主机数 H_{max}，这两个值应当满足如下两个公式：

- 首先：需要划分的子网 $n \leqslant N_{max} \leqslant 2^m - 2$。即求出的 N_{max} 应当大于所需要划分的子网数 n。
- 其次：$h \leqslant H_{max} \leqslant 2^{(t-m)} - 2$，其中，C 类网络的 $t=8$；B 类网络的 $t=16$；A 类网络的 $t=24$。即求出的 H_{max} 应当大于子网中所需要的主机个数 h。
- 本例题目要求为：$n=5$，$h=20$，C 类网络。因此计算如下：

先根据题目要求取 $N_{max} \leqslant 2^m - 2$，由此式求得 $m=3$，最大子网数目为 $N_{max}=2^3-2=6$，满足 $N_{max} \geqslant 5$。

再由 $h \leqslant H_{max} \leqslant 2^{(t-m)} - 2$，$t=8$ 求出 $H_{max}=2^{(8-3)}-2=30$，满足 $N_{max} \geqslant 20$。

结论：经计算对于本例的 C 类网络求出主机编号部分转化为子网掩码部分的位数 $m=3$，N_{max} 为 6，H_{max} 为 30。

ⓑ 求取主机编号部分转化为子网掩码部分的值。

- 将 m 值，按高序依次占用原二进制主机地址的 m 位，并转换为十进制。

例如：本例 IP 为 C 类，原主机编号应为“00000000”，已求出 $m=3$，则有：

$\underline{1\ 1\ 1}\ 0\ 0\ 0\ 0\ 0 \rightarrow$ 224（即主机编号转化为子网掩码部分的值）。

ⓒ 求取最终的子网掩码。

- 对于本例所示的 C 类网络，最终子网掩码应为 255.255.255.224。
- 如果对于 B 类网络，最终子网掩码应为 255.255.224.0。
- 如果对于 A 类网络，最终子网掩码应为 255.224.0.0。

ⓓ 子网编号位为 3，有 $2^3=8$ 种组合，除去表示网络自身的“000”和表示网络广播地址“111”规定不能使用外，共有 $2^3-2=6$ 种有效组合，即在上述网络使用了 255.255.255.224 子网掩码之后，该 C 类网络(202.4.192)可以划分子网的最大数目为 $2^3-2=6$ 个，满足题目 5 个子网的要求。

ⓔ 每个子网中的主机编号为 5 位，因此有 32(2^5)种组合，考虑到主机编号中“全 0”和“全 1”的限制，每个子网中最多支持的主机数目的计算公式如下：

$$2^{(8-n)} - 2 = 2^5 - 2 = 30\text{(台)}$$

由计算可知满足每个子网 20 台主机的要求。

ⓕ 写出求取的 IP 地址最终子网的网络地址和主机编号范围，参见表 7-7。

例如子网 1，因为子网地址为 32，因此，网络中起始的主机编号为 32+1=33，终止的主机编号为“子网地址+每个子网最多主机数目”，即 32+30=62。

综上所述，使用子网掩码划分地址技术，拥有一个可以在 Internet 上使用的 IP 地址的网络，可以根据自身的需要划分成多个子网。本例最多可划分为 6 个。

划分子网时应当注意以下几点：

- 经过划分子网后，一些 IP 地址规定不能使用了，如上述 1 号子网中主机编号“全 0”和“全 1”的地址，例如“202.4.192.32”和“202.4.192.63”等。

表 7-7　子网划分实例的分析计算结果

子网序号	主机编号转化为子网编号部分的二进制数	主机编号转化为子网编号部分的十进制数	子网中 IP 的网络地址	子网中的主机编号	子网 IP 地址初值	子网 IP 地址终值
0*	00000000	0	202.4.192.0	1～31	202.4.192.1	202.4.192.31
1	00100000	32	202.4.192.32	33～62	202.4.192.33	202.4.192.62
2	01000000	64	202.4.192.64	65～94	202.4.192.65	202.4.192.94
3	01100000	96	202.4.192.96	97～126	202.4.192.97	202.4.192.126
4	10000000	128	202.4.192.128	129～158	202.4.192.129	202.4.192.158
5	10100000	160	202.4.192.160	161～190	202.4.192.161	202.4.192.190
6	11000000	192	202.4.192.192	193～222	202.4.192.193	202.4.192.222
7*	11100000	224	202.4.192.224	225～254	202.4.192.225	202.4.192.254

* 说明：虽然标注“ * ”符号的“00000000”和“11100000”的子网为无效子网，但在实际应用中经常被使用。

- 子网掩码的数值，或者是子网的数目，应综合考虑网络中实际需要的子网数目和每个子网中许可的主机数目后再确定。例如：对于本例题，如果需要划分 30 个子网（5 位），则子网掩码为“255.255.255.248”；每个子网中支持的最大主机数目仅为 6 台，就不符合题目要求了。

结论： 由于原有主机编号的位数是固定的，因此，建立的子网数目越多，需要的位数就越多；则每个子网中所能容纳的主机数目就越少。因此，需要综合考虑子网和子网中主机的个数。

④ 划分子网的计算公式如下：

C 类地址：$N_{max} \geqslant 2^m - 2$ 和 $H_{max} \geqslant 2^{(8-m)} - 2$

B 类地址：$N_{max} \geqslant 2^m - 2$ 和 $H_{max} \geqslant 2^{(16-m)} - 2$

A 类地址：$N_{max} \geqslant 2^m - 2$ 和 $H_{max} \geqslant 2^{(24-m)} - 2$

其中：m：为原主机编号部分转化为子网掩码部分的位数；

N_{max}：为转化后所允许的最大子网数目；

H_{max}：为转化后每子网所允许的最大主机数目。

5. 默认网关或 IP 路由

(1) 默认网关和 IP 路由(default gateway 或 IP router)

默认网关又称缺省网关。简单地说，默认网关就是通向远程网络接口的 IP 地址。在子网之间进行通讯时，主机可以使用默认网关将数据发送给目的主机。由于默认网关就是发送给远程网络(目的主机)信息包的地方，因此，如果在配置 TCP/IP 时没有指明默认网关，则通讯仅局限于本地网络。

路由器可以是专门购置的硬件设备，也可以是加装了软件和多个网卡的专用路由计算机。同一个网络段(包含子网段)的计算机之间可以直接通信；不同网络段中的计算机通信时，则需要通过网关或者路由器。其中，内部子网的通信通过内部网关或内部路由器；外部网络之间的计算机通信时一般通过外部路由器(或外部网关)。因此，内部子网与外部网络之间的计算机通信时，需要通过外部路由器(或网关)。下面将通过一个默认网

关应用实例来讲述有关概念。

（2）IP 路由器或 IP 网关的应用实例

两个 TCP/IP 网络之间可以通过 IP 路由器或默认网关进行连接。

① 假定：图 7-2 所示的信息系与自动化系的内部子网掩码均为“255.255.0.0”。

② 问题：如果信息系网络上的某计算机要与自动化系网络上的计算机通信时，如何通过默认网关完成通信过程，参见图 7-2。

③ 解题分析如下：

实例 1　在图 7-2 中，若计算机 A 要给计算机 B 发送信息，由于计算机 A 的 IP 地址是 132.112.000.001，计算机 B 的 IP 地址是 132.112.000.002，所以这两台计算机的网络地址都是“132.112”，由此可知计算机 A 与计算机 B 在同一个网络之内，于是计算机 A 就将信息直接传递给计算机 B，没有经过内部的默认 IP 网关（或 IP 路由器）计算机 L。

实例 2　在图 7-2 中，若计算机 A 要给计算机 X 发送信息，由于计算机 A 的 IP 地址是 132.112.000.001，计算机 X 的 IP 地址是 152.112.000.001，通过其子网掩码求得这两台计算机的网络地址。其中，A 为“132.112”，而 X 为“152.112”。由此可知，计算机 A 与计算机 X 不在同一个网络之内。因此，计算机 A 必须先将信息传递给内部的默认网关（或 IP 路由器）计算机 L 上，然后再由计算机 L 将信息传递给计算机 X。

实例 3　在图 7-2 中，若计算机 A 需要发送信息给 Internet 中的某主机“200.4.192.12”。由于，通过子网掩码求出的计算机 A 的 IP 地址的网络地址与对方主机的不同，A 为“132.112”，而该主机的为“200.4.192”。因此，计算机 A 与该主机不在同一个网络之内。为此，计算机 A 必须先将信息传递给默认的内部网关（或 IP 路由器）计算机 L 上，并由计算机 L 决定是将信息传递给另一子网还是传送给专用的外部路由器。最终，计算机 L 将该信息通过外部路由器发送到外部网络的主机上。

在图 7-2 所示的例子中，只通过一个默认内部网关（或 IP 路由器）和一个外部路由器来传递内部子网间以及与外部网络间的信息，而实际中，由于网络结构比较复杂，因此，可能需要多个默认的内部网关（或 IP 路由器）和多个外部路由器来传递信息。

在对 TCP/IP 的 3 个参数进行配置时，可以进行手动配置 IP 地址，即对其实行静态 IP 管理；也可以使用本章所介绍的 DHCP 服务器对其进行动态 IP 管理。

7.1.4　TCP/IP 的安装与测试

1. **TCP/IP 协议的安装和静态 IP 地址的配置**

若想连通网络，首先应当正确设置网络通信协议。下面以 Windows NT 4.0 为例，简要介绍 TCP/IP 协议的安装和配置，其他各种计算机上有关 TCP/IP 协议的配置与此大同小异。

① 依次选择“开始”→“设置”→“控制面板”命令选项，在“控制面板”窗口中，双击“网络”图标，在打开的窗口中，单击“协议”选项卡。

② 在网络的“协议”选项卡中，单击“添加”按钮，激活如图 7-3 所示的窗口，选中所要添加的协议类型后，单击“确定”按钮，完成添加协议。

③ 在图 7-3 所示的“协议”选项卡中，选中要配置的协议后，单击“属性”按钮，即可对

选中的协议属性进行配置。例如，选中 TCP/IP 协议后，单击“属性”按钮，激活如图 7-4 所示的窗口。

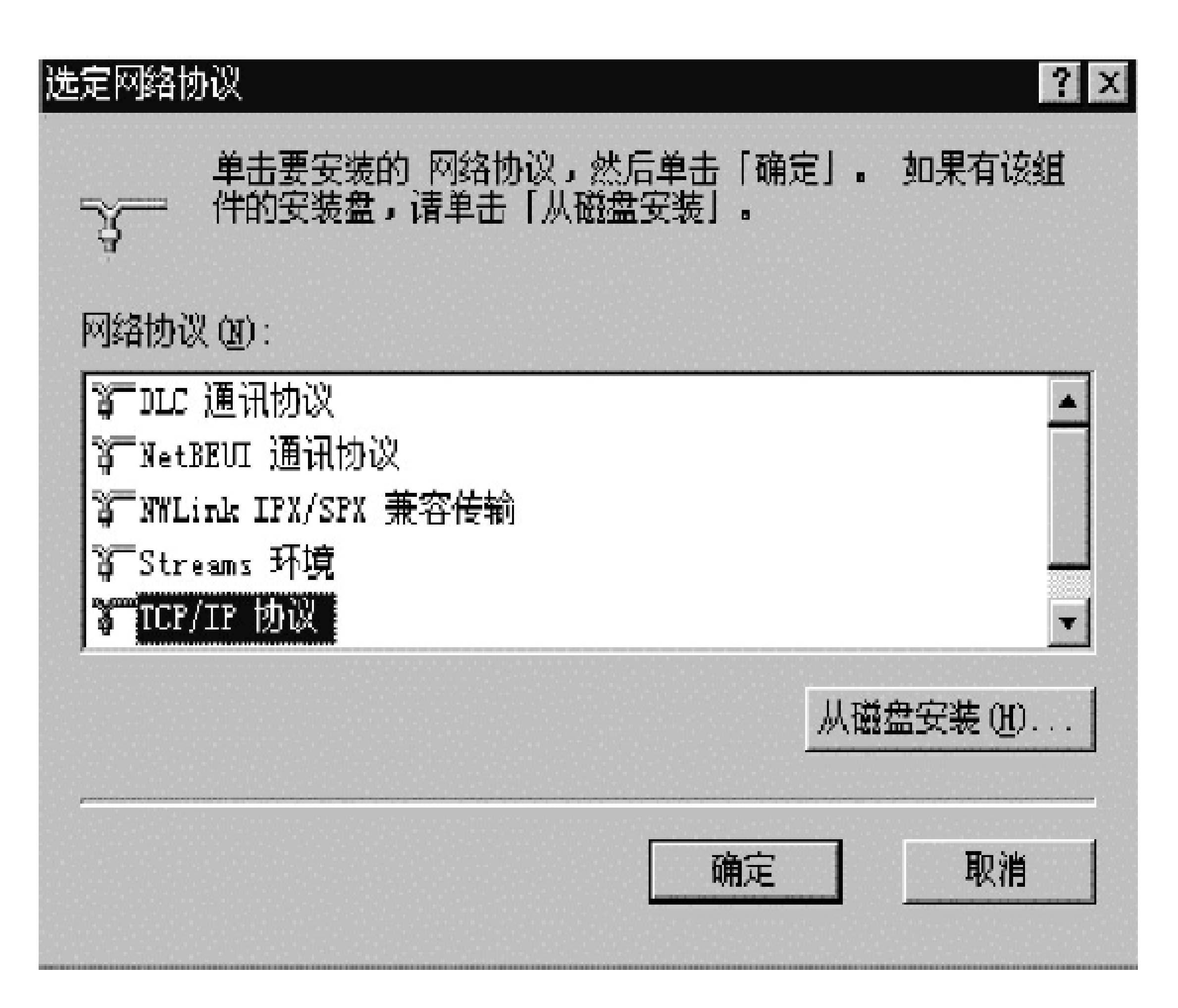


图 7-3 “选定网络协议”类型窗口

提示：由于下面要配置静态(固定)的 IP 地址，所以，在安装 TCP/IP 协议的过程中，如果出现询问“……是否使用 DHCP?”的窗口，应选择“否(N)”按钮。以后，当系统里安装有 DHCP 服务器时，遇到此类情况时，就可以选择“是(Y)”按钮，表示此计算机打算使用一个动态(租借)的 IP 地址。

④ 在图 7-4 所示的窗口中，选中“指定 IP 地址”单选项后，输入分配给该计算机的固定“IP 地址”和“子网掩码”，最后单击“确定”按钮，完成选定 TCP/IP 协议的手工设置过程。

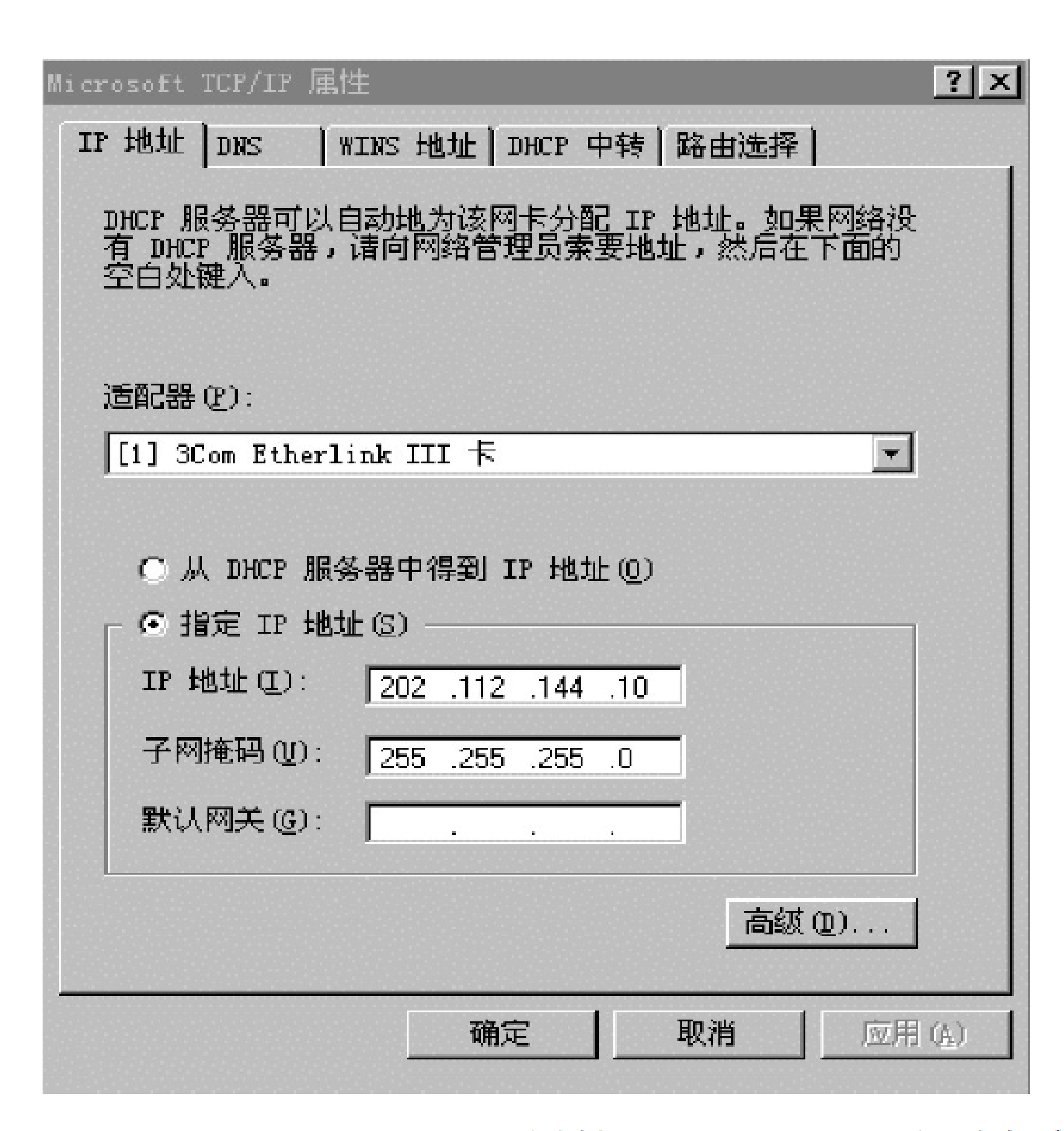


图 7-4 “Microsoft TCP/IP 属性”→“IP 地址”选项卡窗口

2. TCP/IP 协议的测试

网络上的 TCP/IP 协议安装和设置之后,可以使用“ping”命令来进行测试。

ping(packet Internet groper)实用程序是用于测试 TCP/IP 协议配置正确与否的诊断工具。ping 通过向网络上的设备发送 Internet 控制报文协议(ICMP)包,来检验网络的连接性。使用时,大部分设备会返回一些信息,通过这些信息可以判断某一指定的 TCP/IP 主机是否可以正常工作。

启动 ping 程序的方法有 2 种:其一,单击“开始”→“程序”→“MS-DOS 方式”,再输入相应的命令;其二,从 Windows 窗口键入“开始”→“运行”命令选项,再输入相应的命令即可。

TCP/IP 协议的测试步骤如下:

① 验证 TCP/IP 协议是否正确安装。

在 DOS 环境下,利用 ping 工具程序,检查 TCP/IP 协议是否安装,以及其设置是否正确的命令如下:

ping “回送地址(LOOKBACK),即 127.0.0.1”

此命令用以验证 TCP/IP 协议是否正确安装,并正确加载。其中“127.0.0.1”为 LOOKBACK(回送地址)地址。启动 ping 之后,验证正确时将出现如图 7-5 所示的窗口。

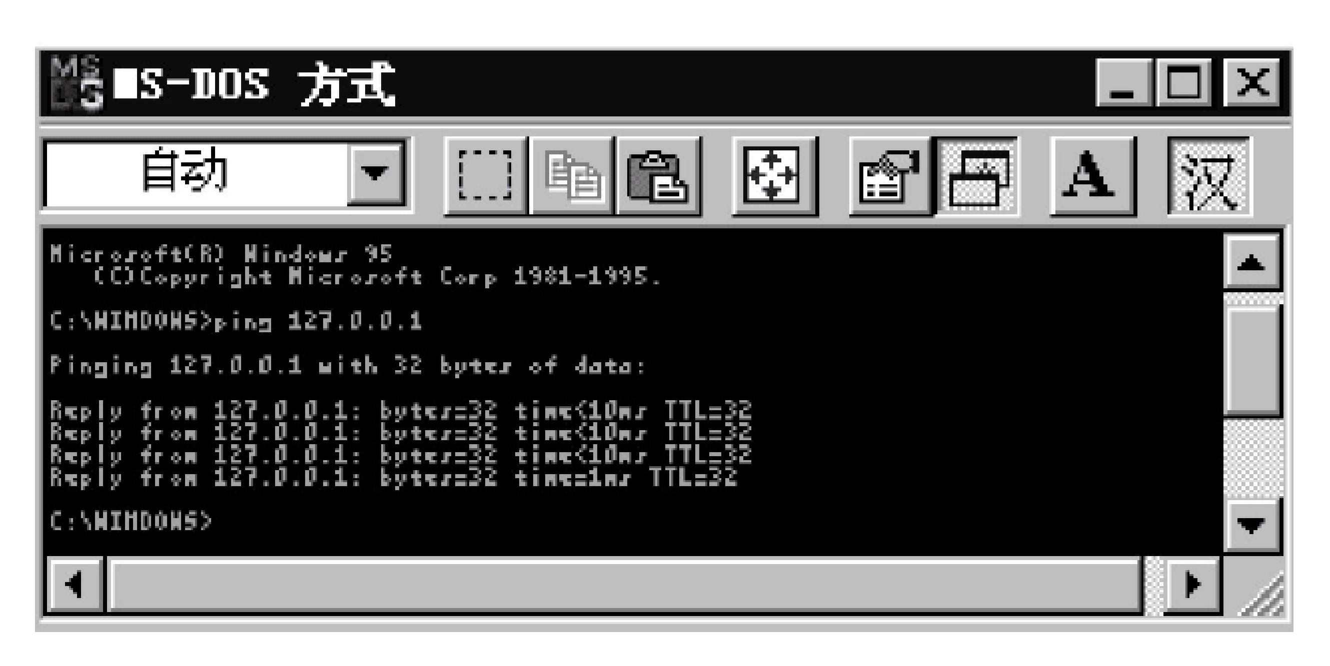


图 7-5　ping 回送地址(127.0.0.1)后正确响应窗口

② 验证网络上计算机主机的 IP 地址是否正确入网。

ping “计算机本机的 IP 地址”(即用户所在计算机的 IP 地址)

执行此命令可以验证该计算机的 IP 地址是否正确加入网中;同时还可以检测网上是否有重复的 IP 地址。例如输入“ping 202.112.144.10”,其中的“202.112.144.10”为用户计算机的 IP 地址。验证正确时将出现如图 7-6 所示的窗口,否则出现与图 7-7 所示的窗口类似的提示信息。

③ 检查网络的连通性好坏验证所测试的主机是否运行正常。

ping “同一网络中其他计算机的 IP 地址”

此命令用以检查网络的连通性好坏,并验证该主机是否运行正常。例如,输入“ping 202.112.144.20”,其中“202.112.144.20”为同一子网上其他主机的 IP 地址。验证正确时将出现类似于图 7-6 所示的窗口,否则出现如图 7-7 所示的窗口。

④ 验证默认网关是否运行正常。

ping “默认网关的 IP 地址”

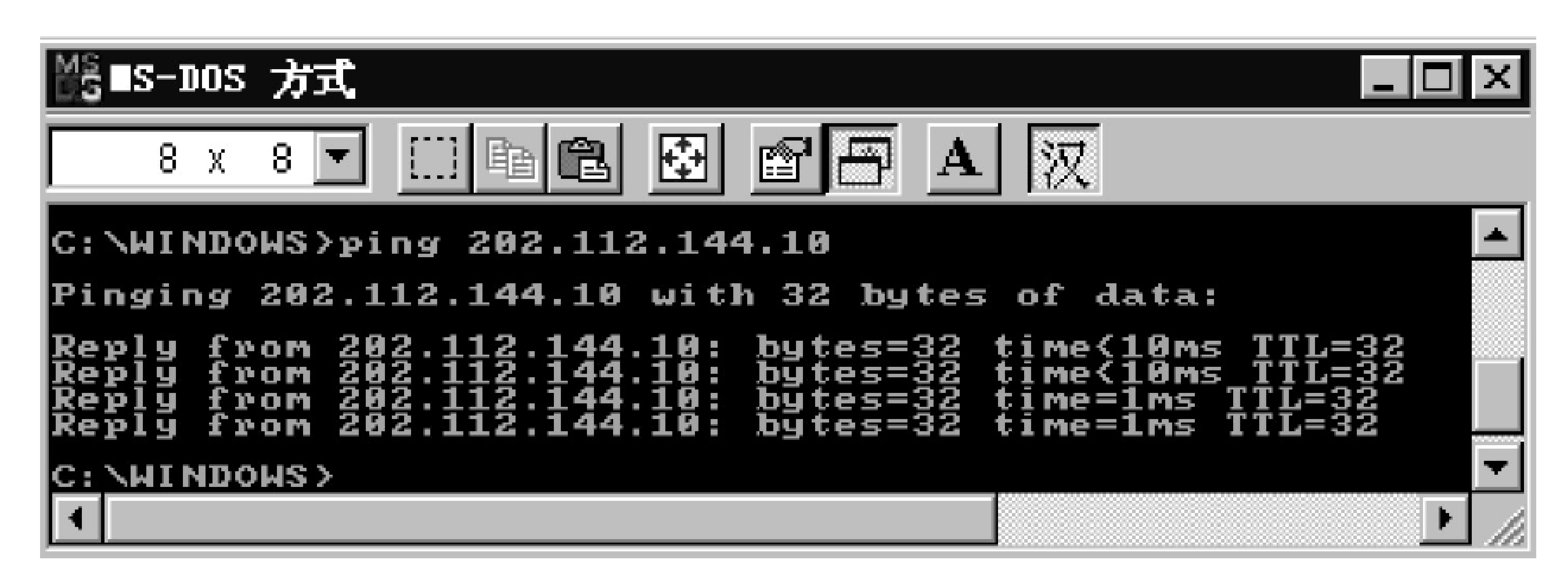


图 7-6　ping 本机的 IP 地址正确时的响应窗口

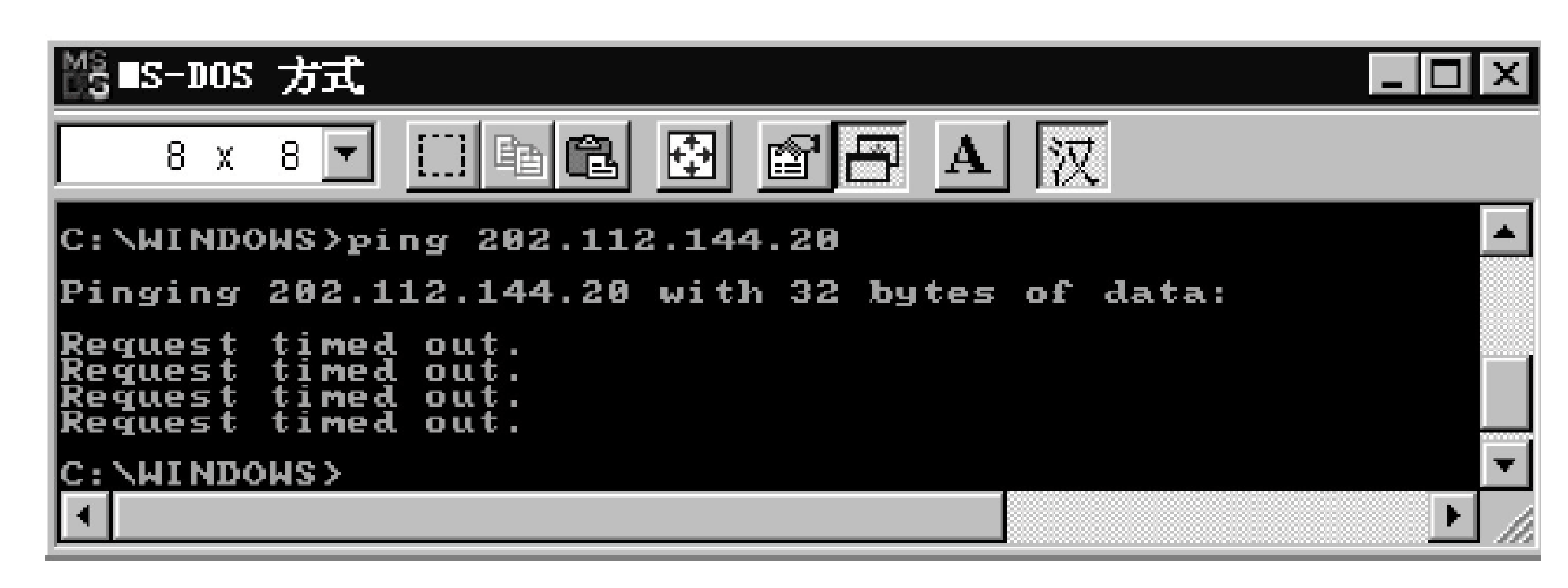


图 7-7　ping 某地址后失败时的响应窗口

此命令用以验证默认网关已经打开,并正确运行,还可以验证是否可以与本地网络正常通讯。如果网络中存在网关机,可用 ping 测试该网关机的 IP 地址。

⑤ 验证所在计算机可以通过路由器(或网关)进行通信。

ping“远程计算机的 IP 地址”

此命令用以验证可以通过路由器(或网关)进行通信。如果网络中存在有使用路由器连接的非本地子网,可用 ping 测试该远程子网上主机的 IP 地址。

技巧:如果从步骤⑤开始检测,并且成功,则步骤①—步骤④都会成功。当然,ping 命令还可用来检测其他网络部件的安装、运行是否正确。

7.2　TCP/IP 协议中 IP 地址的管理

通过前面的学习已经知道,在使用 TCP/IP 协议的网络上是利用 IP 地址来表示网络中的每一台计算机的,为此对于网络中的每一台使用 TCP/IP 协议的主机都必须分配一个惟一的 32 位地址。因此,TCP/IP 协议中的 IP 地址管理主要指 TCP/IP 协议的安装、配置和 IP 地址的分配与管理。

7.2.1　静态 IP 地址和动态 IP 地址

从网络管理的角度看,可以将网络中的 IP 地址进一步划分为静态(固定)IP 地址和动态 IP 地址,其对应的 IP 地址管理又可以分为静态 IP 地址的管理和动态 IP 地址的

管理。

这两种管理方式中，对于不同系统下参数的配置和管理是系统管理员需要解决的主要问题，也是日常维护工作的一项重要内容。

1. 静态 IP 地址

静态 IP 地址是指为一个主机配置的 IP 地址是固定不变的。在较小的局域网中经常使用静态 IP 地址，配置时需要网络管理员或用户对网络中各个主机的 TCP/IP 协议逐一进行手工配置。局域网配置的 IP 地址通常没有什么特殊的要求，而在 Internet 上使用的静态 IP 地址需要到指定的机构去申请。

2. 动态 IP 地址

动态 IP 地址是指一个主机每次连入网时，使用的 IP 地址可以是不相同的，同样可以理解为是系统动态或自动地分配 IP 地址。当网络中主机数目较多时，为了方便管理，通常配置有一个 DHCP(执行动态主机配置协议)服务器，为网络用户提供动态的 IP 地址。各主机连入网络时，向 DHCP 服务器临时租借一个 IP 地址，用过之后会归还给 DHCP 服务器。这种临时租借的 IP 地址，每次的值不一定相同，因此我们称为动态 IP 地址。例如：在 Internet 上，各 ISP 向用户提供服务时，通常同时提供给用户主机一个动态 IP 地址。当局域网中主机数目较多时，通常使用系统配置的 DHCP 服务器为网络用户提供动态 IP 地址。

在 Windows NT 里，使用和管理好这两类 IP 地址是每个网络管理员需要解决好的主要问题。下面以 Windows NT 为例，简要地介绍动态 IP 地址的设置和管理。

7.2.2 动态 IP 地址管理的概述

如前所述对于在 Internet 和 Intranet 上使用 TCP/IP 协议的主机而言，一个独立的 IP 地址是必不可少的，但是，并不是每一个主机用户都能对 TCP/IP 协议进行恰当的配置，许多刚刚开始使用 Internet 的用户，由于对“IP”地址、“子网掩码”和“默认网关”等概念理解不深，在这些参数面前往往不知所措；还有一些用户的计算机需要经常移动，其相应的 IP 地址也必须随之变化。这些 IP 地址的管理和配置问题，都需要系统管理员的帮助和干预。为了解决上述 TCP/IP 参数的管理和配置问题，便引入了 DHCP(dynamic host configuration protocol，动态主机配置协议)。使用 DHCP 的主要原因有以下 3 个：

① 很多普通用户对 TCP/IP 并不了解，因此，不知道如何正确配置这 3 个参数。还有些时候，用户不是从管理员处得到的 IP 地址、子网掩码和默认网关等信息，或是在网络管理员设置之后，自行修改了这些信息，结果将导致很多网络通信方面的问题，当网络很大时，这种问题是很难查找和解决的。

② 管理员或用户在对 TCP/IP 的 3 个参数进行配置时，由于手误，可能将基本参数输错，导致计算机不能正常通信。

③ 由于一些网络客户计算机经常在多个子网间移动，会给网络管理员造成很多管理和配置方面的负担。因为，当客户机处于某一子网时，它使用的 IP 地址必须属于这个子网才能与该网络上的其他计算机通信。当客户机从一个子网中迁移至另一个子网时，必须及时地更改所使用的 IP 地址，方能正常通信。因此，无论在何处，都需要从网络管理员

处得到新的 IP 地址，并重新配置有关的 3 个参数。总之，在工作站上手工配置 TCP/IP 协议时，需要非常仔细地配置 IP 地址、子网掩码和默认网关等信息，只有配置正确的客户机才能与网络上的其他计算机正常通信。

7.2.3 DHCP 服务子系统的工作过程

1. **DHCP 服务器和客户机**

DHCP 服务子系统的工作模式也是客户机/服务器模式。在使用 DHCP 时，整个网络上至少有一台计算机专门用于列出所有可用的 IP 地址、子网掩码和默认网关等信息。我们把这台安装了 DHCP 服务器软件和具有 TCP/IP 相关信息的专用计算机称为 DHCP 服务器。其他使用 TCP/IP 协议的计算机，在启动时会向 DHCP 服务器临时申请一个 IP 地址，并根据 DHCP 服务器提供的信息自动进行配置。这些使用 DHCP 功能的计算机被称为 DHCP 客户机或工作站。使用 DHCP 功能之前，系统管理员必须配置好 DHCP 服务器和客户机，随后，DHCP 服务器将自动解决所有申请、使用和配置 IP 地址等问题。

(1) 对于 DHCP 服务器的要求

① 一般是一台 NT/2000 服务器(server)计算机。

② 具有静态的 IP 地址、子网掩码和默认网关。

③ 在这台 NT 服务器中必须装有提供 DHCP 服务器的相应软件。

④ 有一个 IP 地址池。IP 地址池是指在所有可用的 IP 地址中，划分出的一定范围和数量的 IP 地址，这些地址能动态地分配给 DHCP 客户机(client)使用。

(2) 对于 DHCP 客户机(client)的要求

DHCP 客户机可以是运行目前各种操作系统的计算机，例如 Windows NT/2000 或 Windows 95/98/Me 等。

2. DHCP 的工作过程及所具备的功能

DHCP 的工作过程如图 7-8 所示，主要包括以下几个阶段：

① DHCP 客户机向 DHCP 服务器发出请求，要求租借一个 IP 地址。但由于此时 DHCP 客户机上的 TCP/IP 还没有初始化，还没有一个 IP 地址，因此，只能使用广播的手

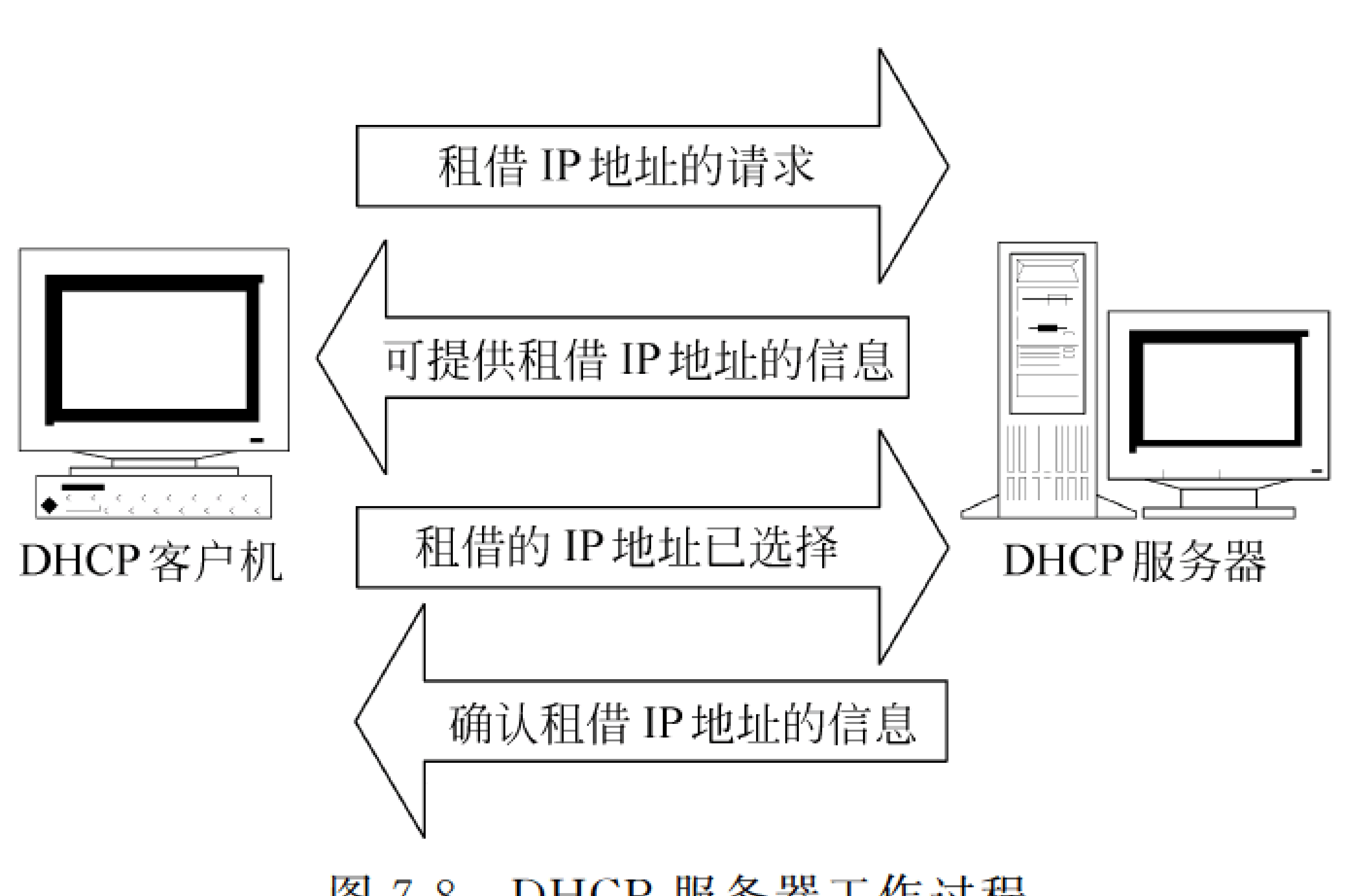


图 7-8 DHCP 服务器工作过程

段，向网上所有 DHCP 服务器发出租借请求。

② 网上所有接收到该请求的 DHCP 服务器，首先检查自己的 IP 地址池中是否还有空余的 IP 地址，如果有，则向该客户机发送一个"可提供 IP 地址"的信息。

③ DHCP 客户机一旦接收到来自某一个 DHCP 服务器的"可提供 IP 地址"的(offer)信息时，它就向网上所有的 DHCP 服务器发送广播，表示自己已经选择了一个 IP 地址。

④ 被选中的 DHCP 服务器向 DHCP 客户机发送一个确认信息，而其他 DHCP 服务器则收回它们的"可提供 IP 地址"的信息。

7.2.4 DHCP 服务器的安装、设置与管理

1. DHCP 服务器的建立

(1) 安装 DHCP 服务器

① 依次选择"开始"→"设置"→"控制面板"命令选项，在打开的窗口中，双击"网络"图标。在激活的窗口中，单击"服务"选项卡，打开图 7-9 所示的窗口。



图 7-9 网络中的"服务"选项卡窗口

② 在图 7-9 所示的"服务"选项卡中，检查是否已经装载"Microsoft DHCP 服务器"，如果没有，单击"添加"按钮，激活如图 7-10 所示的窗口。

③ 在图 7-10 所示的"选定网络服务"窗口的清单中，选中"Microsoft DHCP 服务器"选项，然后单击"确定"按钮进行安装，重新启动计算机后 DHCP 服务生效。

(2) 设置 DHCP 服务器

① 系统重新启动后，依次选择"开始"→"程序"→"管理工具(公用)"→"DHCP 服务器"命令选项，激活如图 7-11 所示的窗口。

② 在图 7-11 所示的"DHCP 管理器"窗口中，选择"作用域"→"创建(C)"命令选项，

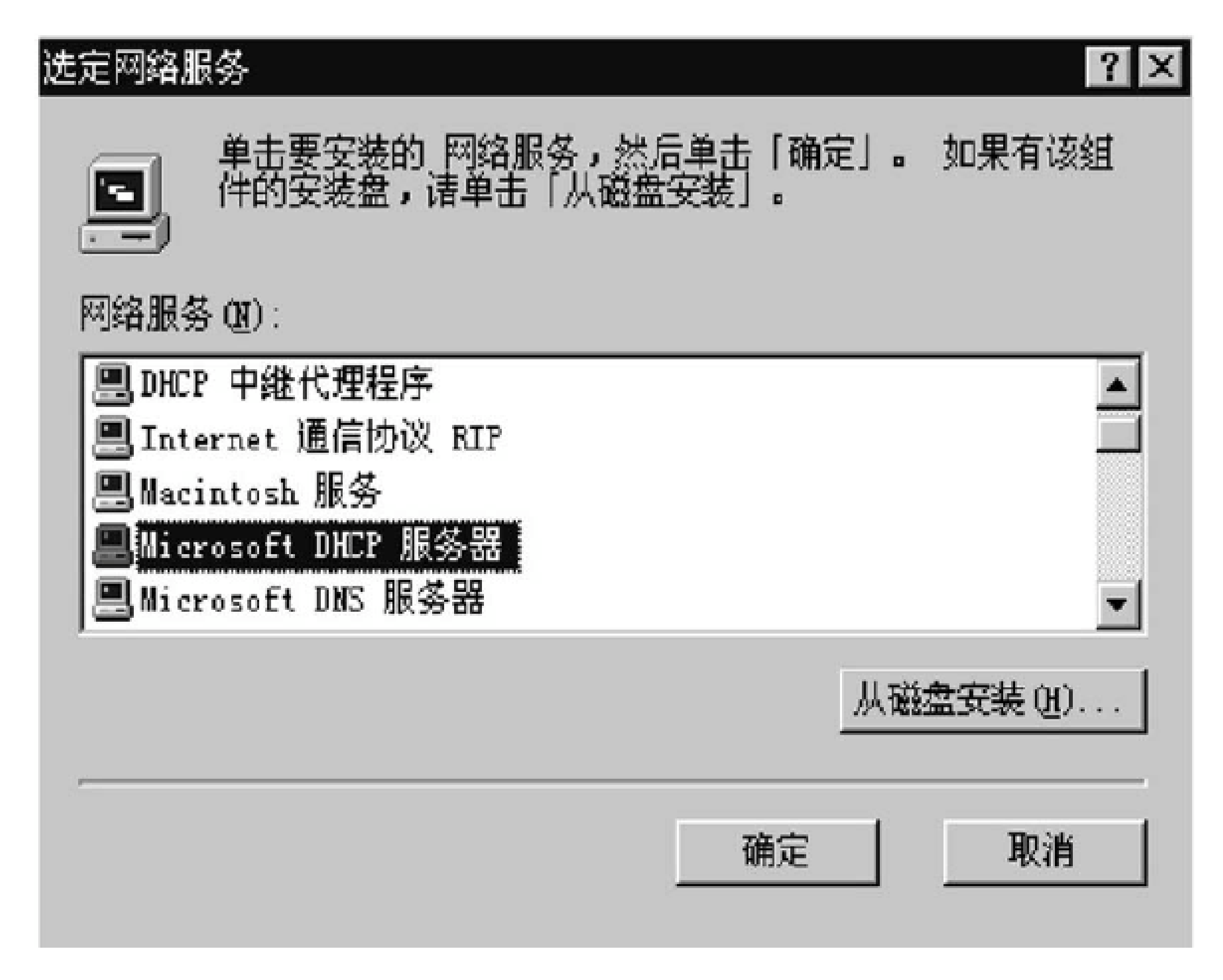


图 7-10　选定网络服务窗口-添加 DHCP



图 7-11　DHCP 管理器

激活如图 7-12 所示的窗口。

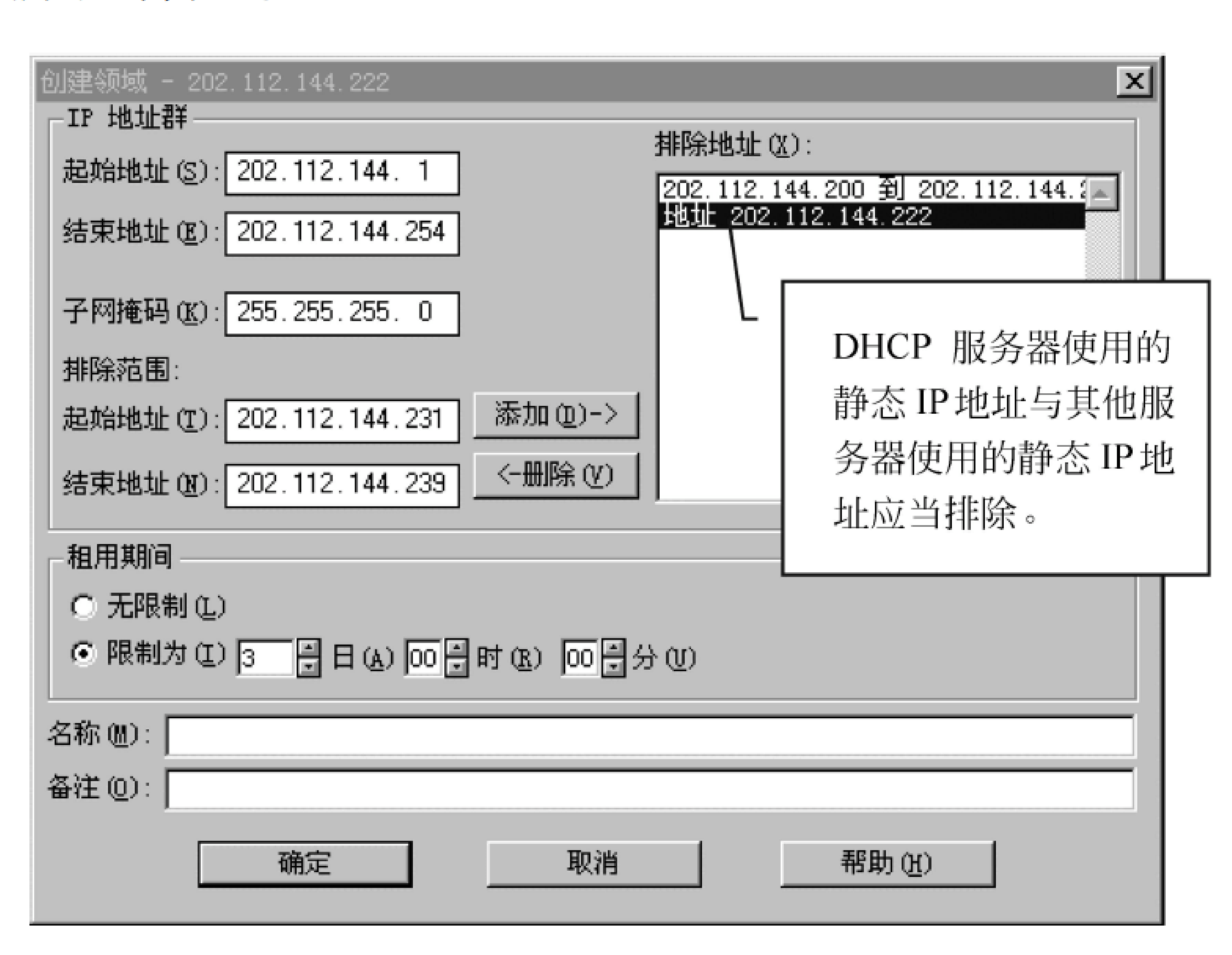


图 7-12　在 DHCP 管理器中打开“创建领域”窗口

③ 在图 7-12 所示的“创建领域”窗口中，对 DHCP 地址池进行配置，也就是建立可用

的 IP 地址范围。当 DHCP 工作站请求 IP 地址时，DHCP 服务器将从此段地址范围中，抓取一个尚未使用(出租)的 IP 地址，并将其分配给 DHCP 客户机使用。图中的 202.112.144.1～202.112.144.254 为可以分配给 DHCP 客户机的地址范围，而 202.112.144.231～202.112.144.239 这段地址另有其他用途，不想分配给客户机使用，所以将其设在“排除范围”内。设置时还应当将 DHCP 服务器使用的静态 IP 地址 202.112.144.222 以及其他服务器使用的静态 IP 地址都设为排除。在窗口中，设置好 DHCP 地址池和子网掩码之后，单击“确定”按钮，完成设置过程。

2. DHCP 服务器上 IP 地址活动租用的管理

(1) 检查 DHCP 服务器上 IP 地址的使用状况

① 依次选择“开始”→“程序”→“管理工具(公用)”→“DHCP 服务器”命令选项，激活如图 7-11 所示的窗口。

② 在图 7-11 所示的“DHCP 管理器”窗口中，选中一个 DHCP 服务器，例如：在选中【202.112.144.222】客户机后，选择“作用域”→“有效租用”命令选项，激活如图 7-13 所示的窗口。

③ 在图 7-13 所示的“活动租用”窗口中，可以查看选中的 DHCP 服务器当前的 IP 地址租用的情况。例如，从图中可知当前客户机的名称为“STATION”，租用的 IP 地址为【202.112.144.225】。

④ 在图 7-13 所示的“活动租用”窗口中，还可以进一步查看当前租用 IP 地址的客户机的情况。例如，选中名称为“STATION”客户机的客户后，单击“属性”按钮。

(2) 断开当前客户租用 IP 地址契约的步骤

在图 7-13 所示的“活动租用”窗口中，要取消客户机的 DHCP 配置时，请在“IP 地址”列表中单击要取消的客户机，然后单击“删除”按钮。例如，选中名称为“STATION”的客户机后，单击“删除”按钮。



图 7-13 “活动租用”→【IP 地址】窗口

7.2.5 DHCP 客户机的设置与管理

安装 DHCP 服务器之后，就可以启用 DHCP 的服务功能，例如，可以在 NT Workstation 客户机和 NT Server 服务器、Windows 95/98/Me 和 DOS 等常用的客户机

上启用 DHCP 的服务功能。

1. DHCP 服务器中的 NT 客户机(非 DHCP 服务器计算机)的设置

Windows NT/2000 客户机上的设置步骤如下：

① 依次选择“开始”→“设置”→“控制面板”命令选项，在打开的窗口中双击“网络”图标，打开如图 7-9 所示的窗口，从中选择“协议”选项卡。

② 在“协议”选项卡中，选中“TCP/IP 通信协议”后，单击“属性”按钮，激活如图 7-14 所示的窗口。

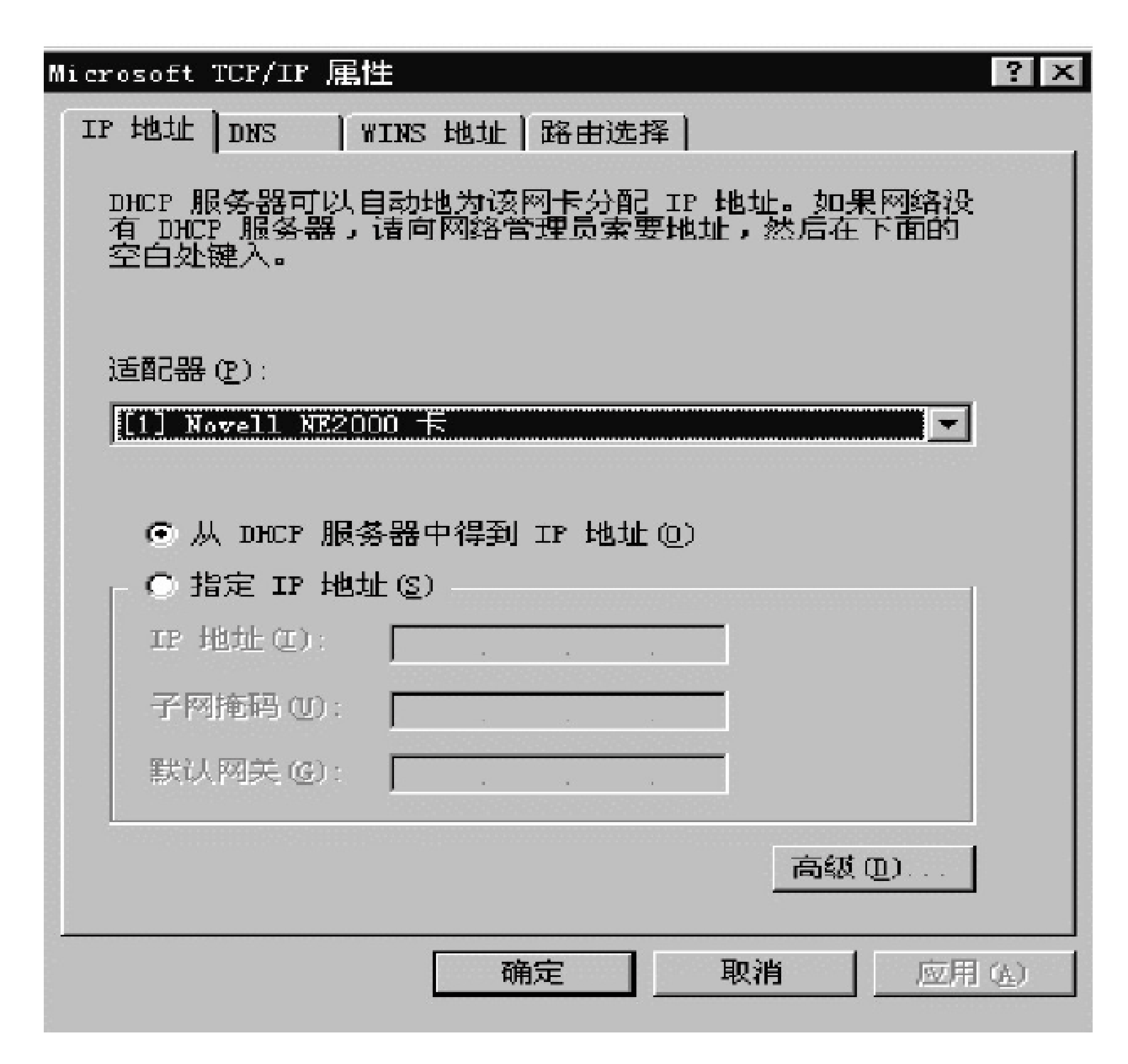


图 7-14 “Microsoft TCP/IP 属性”窗口中的“IP 地址”选项卡

③ 在图 7-14 所示的窗口中，选中“从 DHCP 服务器中得到 IP 地址”单选项后，单击“确定”按钮，完成设置。

2. DHCP 服务器的 Windows 95/98/Me 客户机(工作站)的设置

在 Windows 95/98/Me 客户机(工作站)上的设置步骤如下：

① 依次选择“开始”→“设置”→“控制面板”命令选项，在打开的窗口中双击“网络”图标，打开如图 7-15 所示的窗口，选定“配置”选项卡。

② 在图 7-15 所示的窗口中，选择 TCP/IP→“某类型的网卡”选项，注意：不同类型的网卡此处显示不同。选择后单击“属性”按钮，在激活的窗口中，选择“IP 地址”选项卡，激活如图 7-16 所示的窗口。

③ 在“TCP/IP 属性”窗口中的“IP 地址”选项卡中，选中“自动获得一个 IP 地址”单选项后，单击“确定”按钮，完成设置。

3. “服务器”端和“客户机”端的设置要点

(1) 服务器端

① 在 NT Server 网络上安装 DHCP 服务器，启动 DHCP 服务功能。

② 重新启动计算机。

③ 之后，在 DHCP 服务器窗口中，配置可以租借的动态 IP 地址的范围，以及需要排



图 7-15　网络窗口中的“配置”选项卡

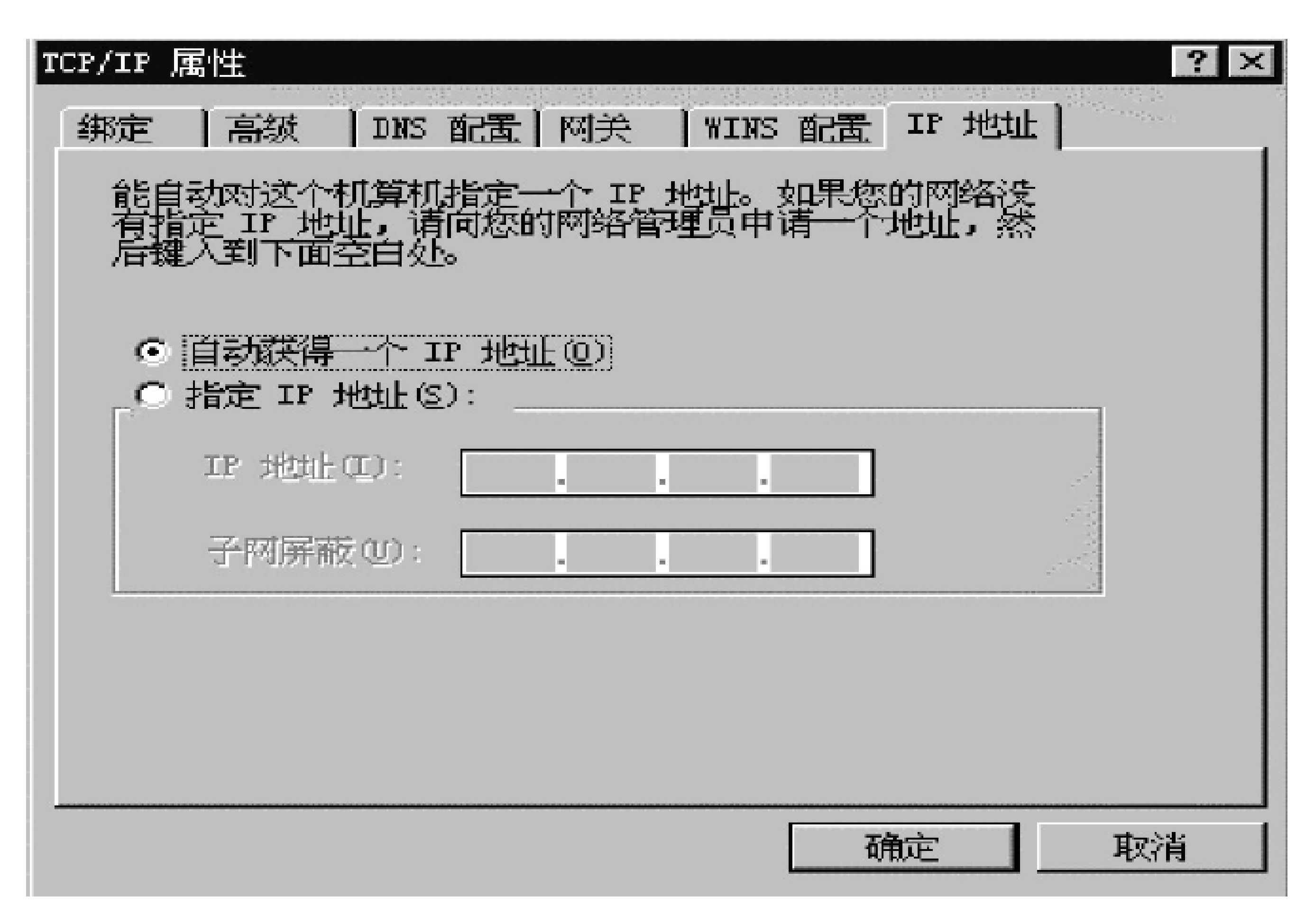


图 7-16　“TCP/IP 属性”窗口中的【IP 地址】选项卡

除的已经使用的静态 IP 地址。

(2) 客户机(工作站)端

① 在 Windows NT 工作站或服务器上安装、配置 TCP/IP 协议的 IP 地址时，选择从“DHCP 服务器获得一个 IP 地址”。

② 在 Windows 98/95/ME/2000 等客户机(工作站)上安装、配置 TCP/IP 协议的 IP 地址时，选择“自动获得 IP 地址”，或者“从 DHCP 服务器上得到 IP 地址”。

习题

1. 选择与填空题

(1) 在下面的 IP 地址中，________属于 C 类地址。

A. 141.0.0.0　　B. 197.234.111.123　　C. 3.3.3.3　　D. 23.34.45.56

(2) 在给主机配置 IP 地址时,可以使用的有:________。

A. 129.9.255.18　　B. 127.21.19.109

C. 192.5.91.255　　D. 220.103.256.56

(3) 在 TCP/IP 参考模型中 TCP 协议工作在________。

A. 应用层　　B. 传输层　　C. 互联层　　D. 主机—网络层

(4) IP 地址中主机部分如果全为 1,则表示________地址,IP 地址中主机部分若全为 0,则表示________地址。

(5) 在 TCP/IP 参考模型的传输层上,________协议实现的是不可靠、无连接的数据报服务,而________协议是一个基于连接的通信协议,提供可靠的数据传输。

(6) 3 类主要的 IP 地址的特征值范围是什么?根据特征值填写下面的表格。

IP 地址特征值范围表

网络类别	IP 地址	网络 ID	主机 ID	网络地址(W)的取值范围	网络个数近似值	主机个数近似值
A	W.X.Y.Z	W	X.Y.Z	1~____	2^7	____
B	W.X.Y.Z	W.X	Y.Z	____~191	____	2^{16}
C	W.X.Y.Z	W.X.Y	Z	192~____	2^{21}	____

(7) 已知 3 台主机进行相互通信时:

它们的 IP 地址分别为:

计算机 A 的 IP 地址:42.211.101.001

计算机 B 的 IP 地址:42.212.101.002

计算机 C 的 IP 地址:41.212.101.001

它们的子网掩码均为:255.0.0.0,试判断并回答:

① 这些计算机分别属于________类网(A、B 或 C)。

② 这些计算机是否属于同一个子网?答:________(是或不是),其网络地址为________。注:若属于同一个子网,请跳答④项。

③ 这些计算机若不属于同一个子网,请回答:计算机________属于同一子网,其网络地址为________;计算机________属于另一子网,其网络地址为________。

④ 这 3 台主机的主机编号依次为:________、________和________。

(8) 在一个 IP 网络中负责主机 IP 地址与主机名称之间的转换协议称为________,负责获取与某个 IP 地址相关的 MAC 地址的协议称为________。

(9) 请为包括两个子网的网络定义网络地址。本题中使用 B 类默认掩码(即 255.255.0.0)中主机编号的两位来划分子网,参见下表。

划分后的 IP 子网掩码			
255 11111111	255 11111111	192 11000000	0 00000000

① 对于 192 所对应的各位填空,并转换为十进制数。

子网掩码第 3 段划分说明	子网编号 2 进制	子网编号 10 进制
无效	00000000	0
子网 1		
子网 2		
无效	11000000	192
		子网掩码第 3 段

② 写出每个子网的网络地址的范围(十进制数)及每个子网的最大主机数。

子网	子网编号初始值	子网编号终值	子网中最大主机数
子网 1	w.x._.1	w.x._.254	
子网 2	w.x._.1	w.x._.254	

2. 简答题

(1) TCP/IP 四层参考模型包含哪些主要协议?

(2) Windows NT 中的 TCP/IP 协议的基本参数有哪些? 各部分的意义是什么?

(3) 如何在 Windows NT 中安装、配置与测试 TCP/IP 协议?

(4) IP 地址中网络 ID 的使用规则有哪些?

(5) 什么是子网掩码? 它有什么用? 如何用它来划分子网?

(6) 在局域网和 Internet 中 IP 地址的使用要求是否一样?

(7) IP 地址分配和使用的基本规则如何?

(8) TCP/IP 协议中 IP 地址的管理包括哪些内容?

(9) 什么是静态 IP 地址和动态 IP 地址?

(10) 为什么要对 IP 地址进行动态管理?

(11) NT Server 中 DHCP 服务器的安装、设置与管理要点有哪些?

(12) 如何在 Windows NT 的客户机(工作站或服务器)上安装、配置动态 IP 地址?

(13) 如何在 Windows 95/98/Me 的客户机上安装、配置动态 IP 地址?

3. 设计与应用题

某个企业目前正在筹划创建企业网络,一方面要将该公司划分几个子网,从而优化网络性能,另外一方面要将自己的内部网络与外部网络隔离。要求:

① 该公司申请到一个可以在 Internet 上使用的 C 类 IP 地址,其网络地址为 202.4.204.0,如果要划分 14 个子网,子网掩码是什么? 每个子网中允许的最大主机数是多少? 请写出分配给每个子网中主机 IP 地址的范围。

② 若每个子网都使用交换式以太网,请画出其中一个子网的拓扑结构图,并标出各设备的名称。

实训题目

1. 在 NT/2000 Server 中建立和管理 DHCP 服务器。

2. 分别在 Windows 95/98/Me /NT 的客户机上完成 DHCP 客户端的设置。

3. 在 NT/2000 Server 中管理 DHCP 服务器,记录和管理有效租用的客户工作站名称。



第8章 网络用户的组织与优化管理

本章主要介绍 Windows NT 网络系统组织结构的特点和基本概念，NT 网络系统组织的优化管理方法，以及网络管理员在建立、管理和维护 NT 网络时应具备的基本技能。

主要内容：

① “域”的组织模式的选择与设计；

② 网络用户的组织与规划；

③ 用户管理中的基本概念和规则；

④ Windows NT 网络组织的优化管理方法；

⑤ 信任(委托)关系的建立与删除；

⑥ NT 网络中的账户管理；

⑦ 用户管理器中的安全规则；

⑧ 用户工作环境的管理。

8.1 Windows NT 中系统组织结构的特点

网络管理员若想管理好一个 Windows NT 网络，首先必须根据本单位网络用户的需求的实际情况，进行网络系统组织结构的规划和设计，只有设计良好的网络结构，再加上必要的网络管理，才可能使网络处于一个良性的运行状态。

Windows NT 网络通常以“域”方式工作，并通过信任关系达到 NT 目录服务的目标，这个目标就是“一个用户，一个账号”(one user，one account)。因此，理解和掌握信任关系，正确建立和使用信任关系，是能否建立和实现整个企业化的网络和安全管理的关键，需要读者很好地体会和理解。

1. 信任关系(trust relationships)的基本概念

首先，管理员应该知道什么是“信任关系”，信任关系指的是资源域(所使用的资源范围)和账户域(账户所在之处)的关系。这就好像我们与自己朋友之间的关系，例如：我信任我的朋友，出差时将自己的大门钥匙给了他，他就可以开门访问我房中的资源。

其次，管理员应掌握如何在 NT 的两个域中使用“信任关系”，并清楚建立信任关系之

后，对两个“域”所带来的影响。

在 NT 网络中，通过使用信任关系来建立两个域之间的通信联接关系。这种联接建立后，其中一个域就赋予了另一个域中的用户以特权，同时允许他们对自己域中的资源进行访问。如果设置正确，当网络中各域之间建立了适当的信任关系之后，用户只要拥有一个账户名称，即可访问整个网络。域中的所有计算机都可以识别这个用户账户。用户登录时只需提供一个账户名称及相应的口令，就可以访问域中的所有计算机。

因此，通过域信任关系的建立，可以将集中式的管理，从“域”级层次提到了企业级层次。在图 8-1 所示的信任关系图中有如下一些基本概念：

① Trust(信任)箭头指向的是“被信任域”，也叫“账户域”，例如信息中心域。

② Trust 箭头从“信任域”(资源域)中指出，资源总是存放在信任域中，例如计算机系统域。

③ “资源域”信任“账户域”中的用户，允许其用户对自己域中的资源进行访问。

④ 跨域赋权。在信任域的基础上，再加上全局组和本地组的管理，使得网络账户管理更加简单。当建立信任关系之后，被信任域中的全局组和全局组用户就可以成为信任域中的本地组的成员。然后，由信任域的管理员，或资源拥有者为此全局组指定访问许可和分配执行管理任务的权限，这就叫作跨域赋权。

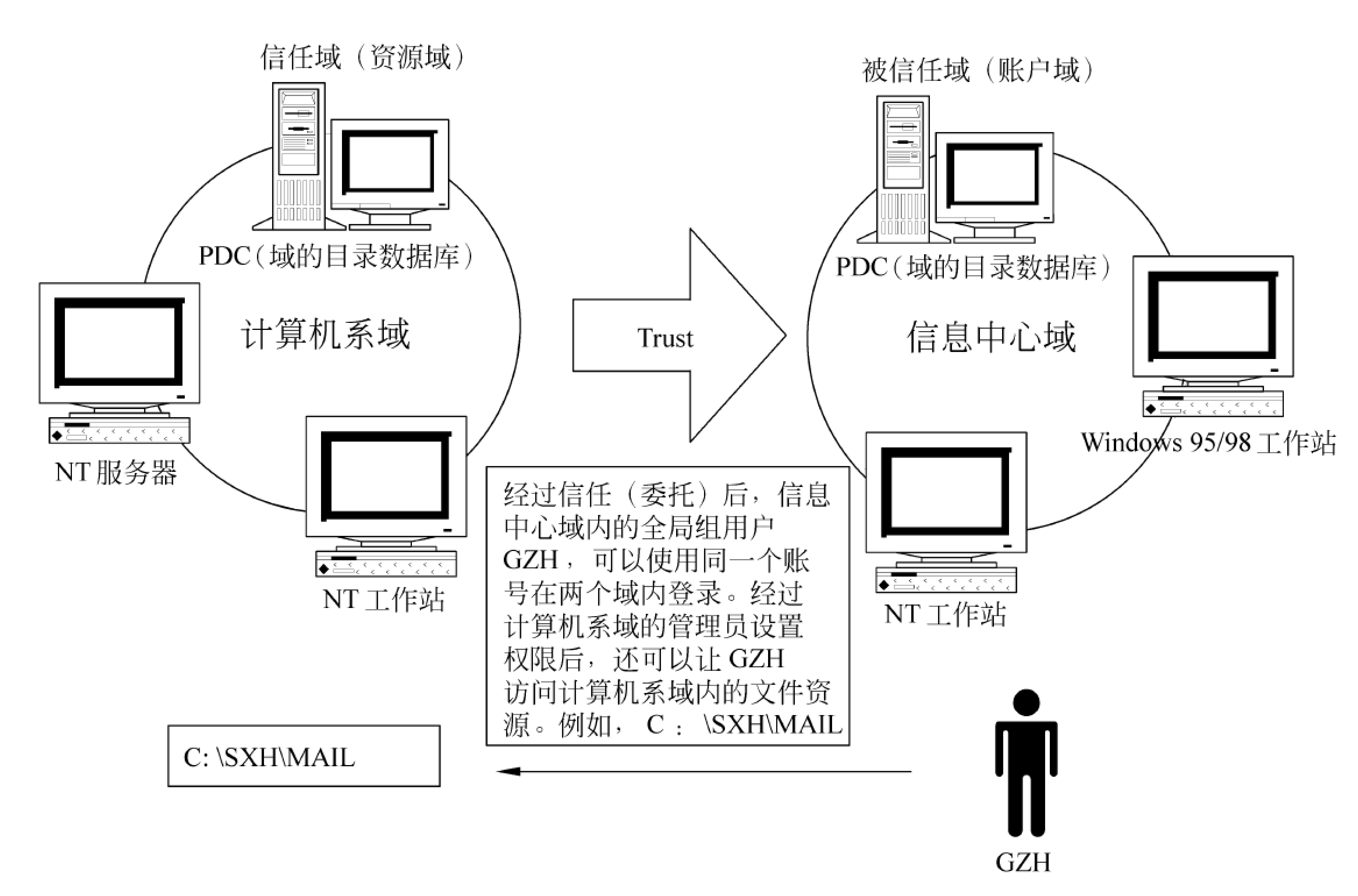


图 8-1　单向信任关系

通过建立域之间的信任关系，把两个或多个独立的域，联接成为一个管理单元。这样，不仅大大降低了管理的复杂性，而且也方便了用户的使用。它使得集中的用户账户管理可以在一个域中进行，而不是分散至各个域中完成。“信任关系”是域间的一种联接，事实上它更像一个网络管理工具，而不是一个用户特征。从账户管理角度来考虑信任(委

托)关系时,可以把信任关系理解为是实现目录服务的手段。如前所述,有了信任关系之后,在资源域中,某用户即使没有该域的用户账号,也可以使用那个域中的资源。

例如:在图 8-1 中,“计算机系统域”与“信息中心域”的单向信任关系建立之后,“信息中心域”中的一个全局用户 WORKGP 经信任与设置权限后,可以同时在这两个域中登录。但应注意,WORKGP 成员从“计算机系统域”中登录 NT 网络时,应在登录用的“输入网络口令”窗口中,输入其在“信息中心域”中的“用户名”和“口令”,在域名处应当输入“信息中心域”。因为 WORKGP 成员是使用“信息中心域”的目录数据库对其用户身份进行验证的,“计算机系统域”中的目录数据库中没有它的账户信息。这样,通过信任关系,就可以实现被信任域“信息中心域”中的 WORKGP 组账户对资源域“计算机系统域”的访问。由此可见,用户物理或逻辑上所处的位置并不重要,而重要的是账户所处的位置。只要用户在被信任域中拥有账户,并能提供相应口令,那么它就可以在任何信任此域的域中进行登录。

2. 单向信任关系

可以利用图 8-1 表示单向信任关系。其信任关系表示,计算机系统域信任信息中心域,使得信息中心的全局组用户 WORKGP 不但可以在本域中登录,还可以在计算机系统域中使用。但是计算机系统域中的账号却不能在信息中心域中使用。

3. 双向信任关系

可以用图 8-2 表示双向信任关系。即 A 域“计算机系统域”与 B 域“信息中心域”互相信任,因此,使得 B 域“信息中心域”的账号可以在本域和 A 域(计算机系统域)中使用。例如:可以在 A 域“计算机系统域”中登录等;同时 A 域“计算机系统域”中的账号也可以在本域和 B 域“信息中心域”中使用。

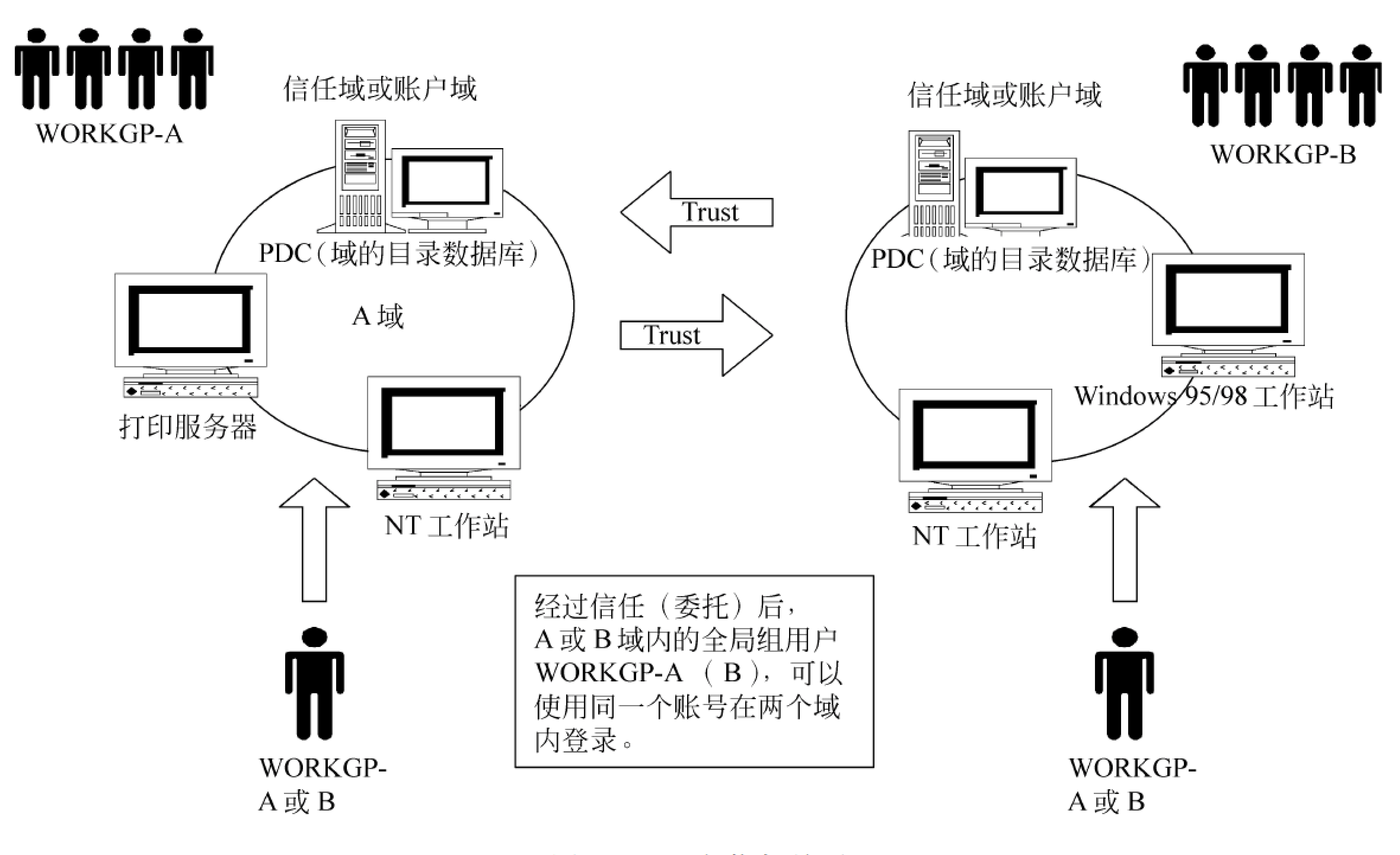


图 8-2 双向信任关系

4. 信任关系不具备转移性(non-transitive)

信任关系具有不可传递的性质。例如:如果 A 域信任 B 域,B 域信任 C 域,但是并不表示 A 域也信任 C 域。域的信任关系通常可以用箭头来表示,即 A→B→C,由箭头的指向可以清楚地看到域的信任关系是不具备转移性质的。虽然,A 指向(信任)B、B 指向(信任)C,但是 A 未指向 C,因此,A 与 C 之间不具有信任关系。也就是说 B 的用户账号可以在 A 中使用,C 的用户账号可以在 B 中使用,但是,C 的用户账号不可以在 A 中使用。

例题:假定 A 信任 B、B 信任 C、C 信任 D、B 信任 D,试问 D 中创建的全局组用户能访问哪些域中的资源?

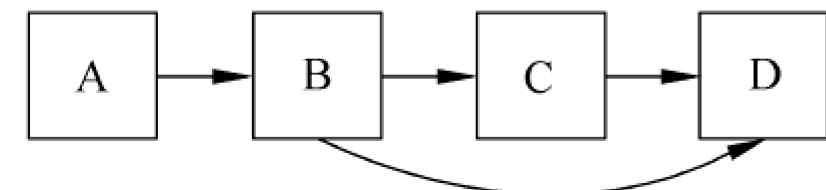


图 8-3　信任关系示意图

解题步骤如下:

① A、B、C、D 之间的信任关系可以用图 8-3 所示的图形来表示。

② 箭头由资源域(信任域)指向账户域(被信任域)。

③ 被信任域全局组的用户可以使用信任域中的资源,在图 8-3 中,可以清楚地看到只有两个箭头(B 和 C)是指向 D 的。因此,在 D 中创建的全局组用户能访问的外部域只有 B、C 两域,加上自身域 D,故 D 中创建的全局用户能访问的域为 B、C 和 D。

5. 信任关系中的传递验证

用户通过传递验证使得他能够登录到网络中的他不具备账户的计算机或域中。因此,用户通过传递验证和域与域之间建立起的信任关系,就可以只在某一个域中拥有一个账户就能访问整个网络。

如果用域 A 代表计算机系域,用域 B 代表信息中心域,WORKGP 是域 B 中的全局组,则在图 8-1 中所示的“传递验证”的应用过程如下:

① WORKGP 中用户 GZH 的 NT 计算机和域控制器开启,同时它的网络登录服务启动。

② 域 B 的 WORKGP 用户 GZH 想登录到域 A 中,但他使用的是域 B 中建立的用户账号。

③ 域 A 的主域控制器不能够验证该 WORKGP 的用户 GZH 账号,因为域 A 的目录数据库中无此信息。

④ 验证请求通过信任关系,从域 A 传递到域 B 中,域 B 的主域控制器接受该请求,检查自己的目录数据库,并对该用户 GZH 账号的身份进行验证。

⑤ 域 A 的域控制器将返回的验证信息传到 WORKGP 用户 GZH 登录的域 A 中的计算机上。

至此完成登录过程。由此可见,当被信任域的用户在信任域中的某台计算机上登录时,或者当被信任域的用户访问信任域中的资源时就会发生传递验证。

8.2　“域”的组织模式的选择与设计

在构造 NT 网络系统之前,应当做好域的规划工作,这决定了网络日后的使用与维护的难易程度。下面将介绍几种域模式读者可以此作为参照,来组织和设计自己的计算机

网络系统。设计一个“域”的组织模式时应考虑以下一些问题：

- 需要使用网络的用户数量；
- 需要使用网络的用户所处地点，应尽可能地实现账户的集中管理；
- 企业的类型以及组织情况；
- 用户所要访问的资源情况，例如类型、数量、地点和管理方式等。

在考虑上述问题的基础上，可以从以下几种域的组织模式中，选择一个合适的模型作为自己企业的域管理模式。

8.2.1 “单域”模型

1. “单域”(single domain model)模型特点

Windows NT 目录服务“单域”模型将所有账户和资源放在同一个管理单元中，使得“一个用户，一个账号”的概念和目标得以实现。在“单域”模式下，所有用户账户和全局组都在同一个域中，无需使用信任关系，这种模型非常简单，对于那些用户数量不多(一个域可支持高达 26 000 个用户账号，至于准确的数目应根据域中的服务器数目和硬件配置的情况酌情而定)，并且希望账户和资源集中管理的公司，“单域”模型是最佳选择。目前，许多小企业或小单位都采用这种结构，如图 8-4 所示。



图 8-4 “单域”模型

如果用户的网络上有许多服务器，或是单位内有许多部门，那么这种“单域模型”就不一定是最佳的选择。这时，最好将网络有组织地分成多个域，使得资源的查找更快速和更有效。

2. 适用范围

小型工作室、小型企业、小型单位和学校计算机实验室内的简单网络系统使用单位。

8.2.2 “单主域”模型

1. “单主域”(single master domain model)模型特点

在“单主域”模式下，NT 的目录数据库通过信任关系来实现域之间的联接，使得“一个用户，一个账号”的目标在多个域环境下也能实现，如图 8-5 所示。

在“单主域”模型中，至少有两个域，每个域都有自己的主域控制器。但所有的用户账户和全局组的信息都保存在主域的域控制器上。“主域”又叫做账户域，也是被信任域，所有其他的域都信任主域。这是由于，所有的用户账号都建立在“主域”中，因此其他域必须信任“主域”，其他域都叫做“资源域”。在此模型中，能够实现账户的集中管理，但资源管理却是分散的。

对于一个按部门和区域进行分类，并且各部门各地区希望能独自进行资源管理，同时又希望整个公司的账户集中管理的公司，采用单主域模式最为适合。

在“单主域”模型中，组的管理也是非常重要的。为了简化管理，资源域的管理员需将主域中的全局组放到资源域中的本地组中，并对本地组指定相应的权限和许可。而在主

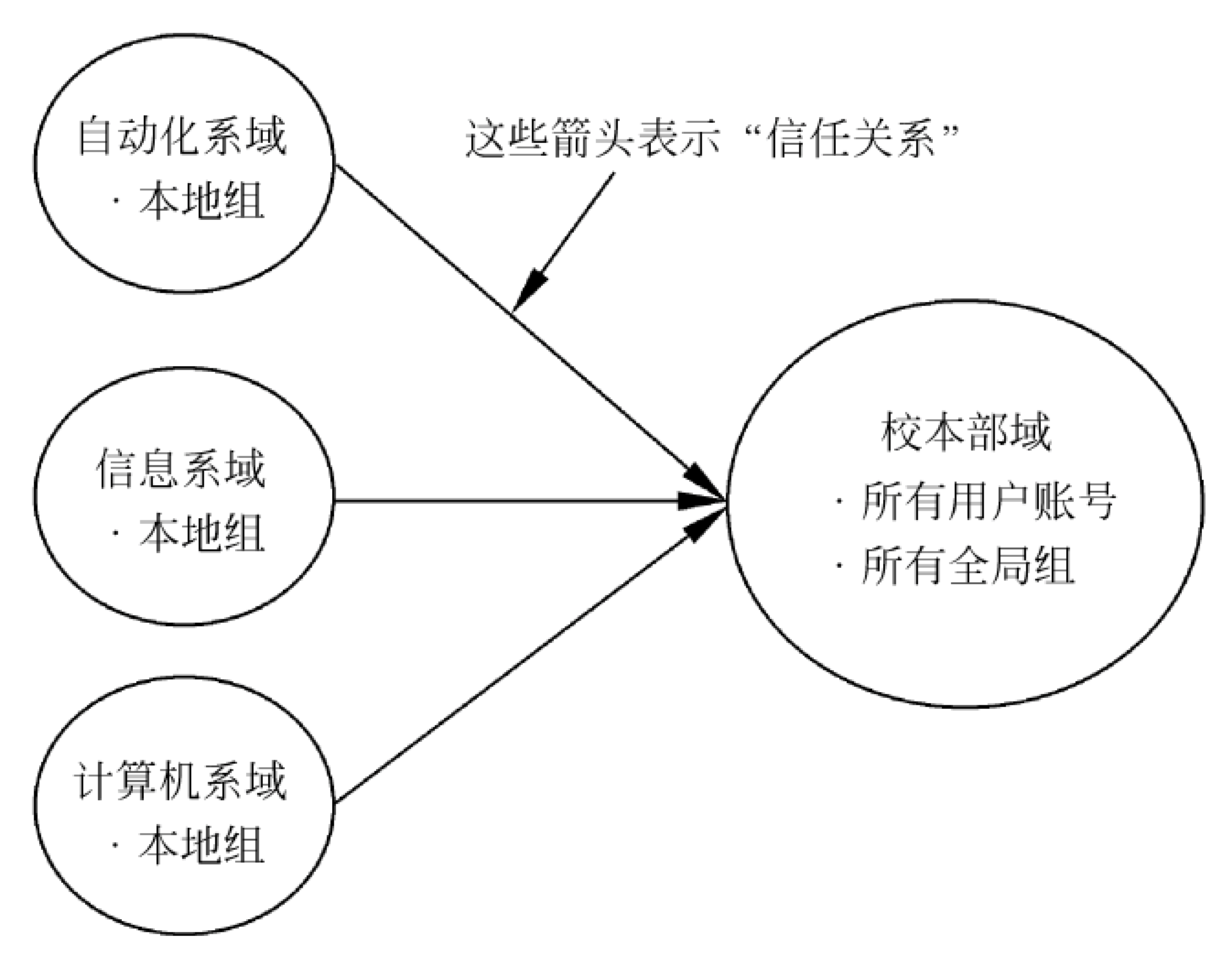


图 8-5 “单主域”模型

域中，管理员仅仅需要把用户账户加入到合适的全局组即可。

2. 适用范围

“单主域”模型适合于网络用户不多，但是由于组织规划的原因，需将网络分割成多个域的场合。此模式同时提供了账户的集中管理与组织的功能。例如，中型企业、中型机关单位和学校管理系统等内部需要多个独立部门时，适合使用“单主域”模型。

8.2.3 “多主域”模型

1. **“多主域”**(multiple master domain model)**模型特点**

“多主域”模型如图 8-6 所示，它是“单主域”模型的一个扩展，如果信任关系建立得当，用户也能通过传递验证，使用一个账号和密码从任何一个域中登录。

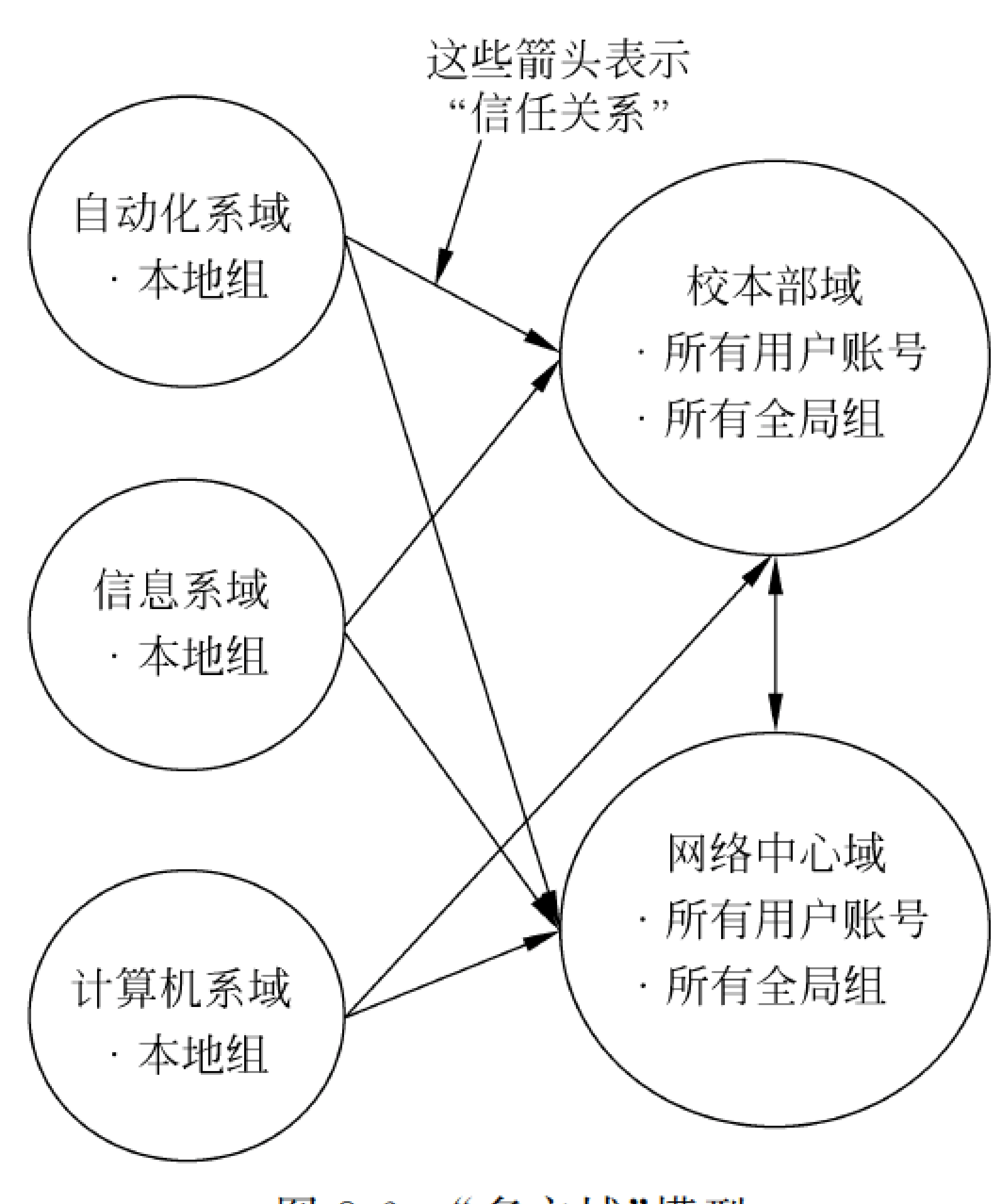


图 8-6 “多主域”模型

在“多主域”模型中，每一个“主域”都通过双向信任关系和其他“主域”建立联接。每一个资源域都信任“主域”，但并不信任其他资源域。对一个要求有多个管理单元的跨国大公司，“多主域”模型是最佳选择，在每个管理单元中，管理员都能完全控制自己的账户。对于组账户的管理，“多主域”模型和“单主域”模型完全相同，只不过需要在每个“主域”上都创建全局组。

2. 适用范围

“多主域”模型适合于配备大型网络，且需要集中管理的公司。顾名思义，这种模式由多个“主域”组成，同时所有的用户账号分别建立在这些“主域”之中，并且每个用户在整个网络上只需要一个账号，不需要在每个“主域”上都建立一个账号。例如：大型企业、跨国公司和国家部门等单位适合使用“多主域”模型。

8.2.4 Windows NT 如何识别域

如前所述，网络用户是利用域的名称来访问域的。但是在 NT 内部却是利用域的安全标识符(security identifier，SID)来确定一个域的。域的 SID 是在安装 PDC 与 BDC 的过程中产生的，它是惟一的号码，不会与其他域的 SID 重复。

在 PDC 和 BDC 中，域名和域的 SID 是不等价的。一个域的域名可变，但域的 SID 不可变，域名变化后，新的域名将和原有的 SID 相结合。正是由于域 SID 的惟一性，因此，如果不经重新安装 PDC 和 BDC，就不能改变其 SID，也就是说不能将一个域的 PDC 迁移到另一个域，并取代那个域中的 PDC。而普通的 server 和 workstation 也拥有自己的 SID，这个“SID”是指计算机的 SID，因此只用来标识一台计算机。所以，它们可以不必重新安装，就从一个域迁移到另一个域中。因此，对于“单主域”和“多主域”模型中的每个域的 PDC 都应当分别安装，而不应使用硬盘克隆、硬盘对拷和镜像安装等快速安装方法。

8.3 网络用户的组织与规划

当完成了网络的总体规划和“域”模式的设计以后，应该根据域的组织模式，对各部门需要建立的组和用户账号进行总体规划设计，从而完成对“组”和用户账号的建立和管理工作。网络的用户管理是网络系统管理中的一个重要环节。当前许多单位都建立了 NT 网络，但在实际的管理和使用中普遍存在的问题是，网络系统中的多个组和用户处于杂乱无章的状况，系统资源的管理无序，用户权限没有设定，安全访问控制机制没有建立，因此，存在着十分严重的安全隐患，系统管理十分薄弱。

8.3.1 用户管理中的基本概念和规则

1. 账户管理中的基本概念

在建立(添加)和管理账号以前，应正确理解以下几个基本概念：

(1) 用户(user)

用户指的是一个实实在在的人，计算机的使用者。正像一个人可以拥有多个银行账

户和密码一样，一个用户也可以有一个或多个账号及密码。

(2) 用户账号(user account)和密码(password)

当某一用户需要登录上网时，必须向管理员申请一个用户的账号(账户)，而后每次上网登录时，需要先输入账号和密码(如果设置了的话)，经验证合格后，方可进入网络。NT具有很强的安全保证能力，因此，只有系统的合法用户，才能在NT系统中登录，而这种登录的权利是事先授予的。在NT域中，每一个用户账号包含了该账号的所有信息，例如：用户名(即用户账号)、口令、所属的组以及允许用户使用的系统资源权限等。

(3) 用户权限(user right)

为了保障系统资源的安全性，在域系统中，用户存取数据与使用共享资源应当依据所拥有的权限来进行。所以，域的管理者应当为每一个用户赋予适当的操作权限，这样才能实现对数据或共享资源的访问控制。

(4) 建立账号的最小特权原则

账户管理中有一个"最小特权原则"，这个原则指的是给一个用户建立多个账号，每个账号在NT的安全系统中具有不同的特权和能力。在执行不同的任务时，仅使用能够完成该任务的具有最小特权的账号。对管理员账户来说，最小特权规则尤为重要。因此，系统管理员应当为自己设置和建立起多个用户账号，在执行不同的任务时，仅使用能够完成该任务的具有最小特权的账号，这样做才比较安全、合理。

2. 利用组账户管理账户的概念

(1) "组"(group)与"工作组"

"工作组"与"组"的概念不同，前者是指网络中计算机的一种组织方式，而"组"是在网络中为了方便管理，而在"域"或者"工作组"中引入的一种内部管理组织。管理员通常将每一个"域"划分为多个方便管理的"组"，性质相同的用户被分配到同一个组，并通过对"组"设置权限而实现对用户赋权，从而方便了系统管理。

(2) 组账户的特点

利用"组"管理用户账号时，需要使用到"组账号"的概念。

① 组账号是用户账户(账号)的集合。所谓"组账号"就是包含组中所有成员用户的账号。实际操作时，应先创建"组"账号，再添加该组各成员的账号。

② 赋予"组"的权限和许可时，对于"组"中的所有成员都会生效。因此，使用组账号可以方便和简化管理。可以将性质相同的用户归到一个组中，然后对此组的权利进行设置。而后，无须对组中的所有用户分别进行设置，组中的用户就同时拥有了这项权利。例如：自动化班级的名称为ZDH9831，共有35名用户，为了管理方便，可以将这35名用户归为ZDH9831这个组。当为ZDH9831组设置了对系统中"\9831"目录具有"只读"的访问权利时，这35名用户就都享有了同样的权利，而不必依次对这35个用户赋予这项权利。

8.3.2 Windows NT 网络组织的优化管理方法

本节将对如何通过合理和优化的方法，设计和实现一个合理的网络用户管理结构作重点介绍；并在此基础上，讲述为用户分配和划分访问权限的内容。网络用户的组织、规划和实施步骤可以分为以下几个基本部分：

1. 确定网络中“域”的组织模式

在构造局域网络的用户系统之前,应当首先对网络需求进行调查,再确定网络中“域”的组织模式。因为,域规划工作的好坏决定了网络日后的使用与维护的难易程度。

下面以某校为例,简要介绍网络的组织和规划工作,用户可以此作为参照,来组织和设计自己的计算机网络系统。在对该校实施网络管理之前,首先应对该学校的各个部门及其成员情况进行分析,然后,再进行域、组和账户的规划和设计。设计这个网络系统的组织模式时应考虑以下一些问题:

(1) 单位的类型以及组织情况

假定某个学校有多个部门,该校的主要部门是自动化系(2 个用户为代表)、信息系(2 个用户为代表)、计算机系(2 个用户为代表)和网络中心(3 个用户为代表);另外,学生域中按班级设立组账号。

(2) 需要使用网络的用户所处的地点

假定这些用户和组的成员都在本地,因此,没有远程登录账户。

(3) 需要使用网络的用户数量

根据上述部门的情况,假定用户数量为教师和管理人员账户 9 个,班级账户 2 个。

(4) 确定网络中“域”的组织模式

在考虑上述问题的基础上,已选择了 Windows NT 作为网络操作系统,并选择“单主域”的组织模式作为自己学校的域管理模式。该校按主要部门划分为域,即“自动化域”、“计算机系域”、“信息域”、“学生域”和“网络中心域”。主域为“网络中心域”,它负责并进行全网的统一管理,上述的各部门域均信任主域。其中,网络中心又分为软件组、硬件组和系统维护组,他们分别负责整个 NT 网络的软件、硬件和系统的技术支持工作。

(5) 确定使用者的管理方式

由于在每个单位中,每位员工的分工不同,所属部门不同,对资源的需求不同,所以,管理员应当根据用户所要访问的资源情况,例如类型、数量、地点和性质等,确定需要的组账号的数量以及各组账号管理和用户账户对资源和网络的访问权限。第 1,对于某公司的人员分工来说,有经理、中层管理人员和一般职员,他们所用的账户各不相同。第 2,对于用户所属的部门来说,有研发部、财务部、市场部和网络信息管理部等多个性质不同的部门,每个部门需要使用的网络资源也不同。第 3,同一部门中的每个人,对网络资源的使用要求也不同,例如,对普通人员需要能够“读”信息,而对于部门领导则可能需要“写入”的权限,而对于网络管理人员来说可能需要具有所有的权限。因而,管理员应当对网络系统中的所有用户、组、资源和权限进行精心的组织与设计。

2. Windows NT 网络中的访问权限

Windows NT 网络提供的针对用户和组账号对“域”的访问权限共有 11 种,参见表8-1。

3. 组的设计原则

利用“组”管理用户账号,创建组时需要考虑的原则如下:

① 根据共同的需要从逻辑的功能出发组织用户。例如,所有学生需要共享激光打印机,则可以通过建立“学生组”来组织学生用户;而所有教师需要访问学生的数据库记录文件,则可以通过“教师组”来组织教师用户。

表 8-1　用户和"组"的对"域"的访问权限编码表

编号	权限编码	权　　限
1	A	还原文件和目录
2	B	在"域"中添加工作站
3	C	关闭系统
4	D	取得文件或其他资源的所有权
5	E	从网络上访问此计算机
6	F	从远端系统进行强制关机
7	G	备份文件和目录
8	H	在本机登录
9	I	添加、删除和修改外部设备驱动程序
10	J	管理审核与安全日志
11	K	更改系统事件

② 在每一个用户账户所在的域中，为每个逻辑组的用户创建一个全局组，然后将适当的用户账户放入相应的全局组中。例如，在主域中创建全局组 wh，然后将所有维护组的用户账户放入该组中。

③ 还可以根据访问资源的需要创建本地组。例如，网络中心各组的网络管理人员需要对"C:\WINNT"目录中的文件完全控制；而自动化系的教师对该目录中的文件，只需要读的权限。因此，可以给网络中心各组创建一个本地组，而给自动化系的教师创建另一个本地组，并分别赋予它们不同的访问权限。对于上述组的说明如下：

- 如果资源的位置在成员服务器或者 NT Workstation 的计算机上，则应在资源所在计算机上创建本地组。
- 如果资源的位置在 PDC(主域控制器)或者 BDC(备份域控制器)上，则应在 PDC(主域控制器)上创建本地组。

④ 给本地组分配合适的许可。

⑤ 将全局组加入本地组。应当注意：当将一个域的全局组加入到另一个域的本地组时，必须先建立起合适的信任关系。

4. 网络用户的组织与规划

根据上述实例中用户的特点，对该校的 NT 局域网的用户进行组织和规划。组织和规划的内容包括：域规划、组规划、信任关系规划和用户规划等几个方面。

(1) 域和信任关系的规划

① 自动化系为一个"域"，名称为 ZDHDOMAIN，单向信任主域名称为"NETDOMAIN"的网络中心域。

② 信息系为一个域，名称为 XXDOMAIN，单向信任主域 NETDOMAIN。

③ 计算机系为一个域，名称为 JSJDOMAIN，单向信任主域 NETDOMAIN。

④ 学生设为一个域，名称为 STUDOMAIN，单向信任主域 NETDOMAIN。

⑤ 网络中心为一个域，名称为 NETDOMAIN，通过建立单向信任关系设置为"主域"。信任关系图与图 8-5 类似，即 ZDHDOMAIN、XXDOMAIN 和 JSJDOMAIN 各域都

信任主域 NETDOMAIN，即网络中心域。

（2）“组”和用户账号的规划

① 绘制 NT 网络的管理目录“树”。

根据前面的规划设计原则，对该校的“域”、“组”和“用户账号”的设置规则是，先对实例中学校里的各个“域”进行了规划；其次，对组进行规划设计；最后，绘制系统的规划管理目录“树”，参见图 8-7。

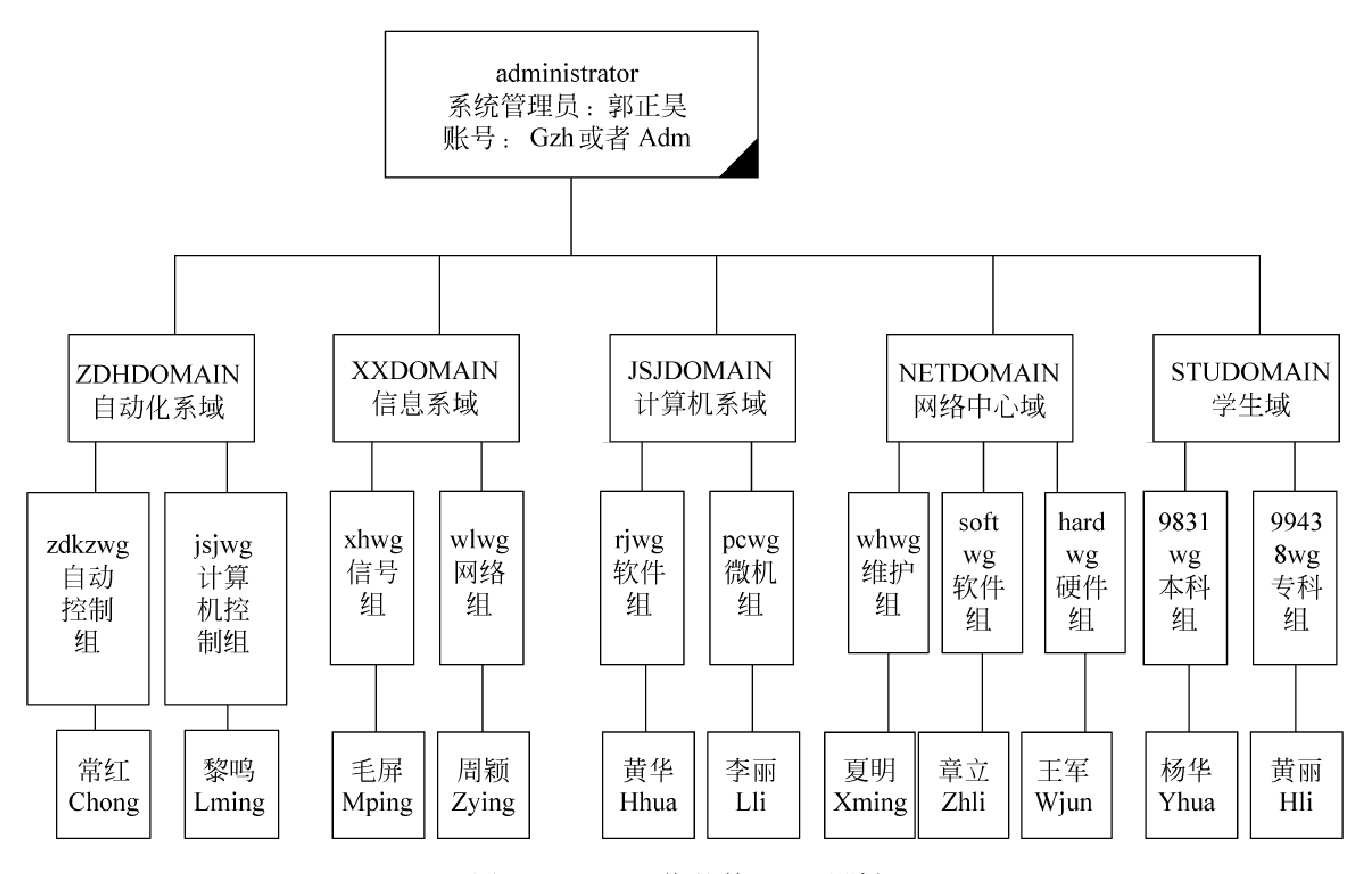


图 8-7　NT 网络的管理目录“树”

② 确定 NT 网络的管理明细清单。

如图 8-7 所示，根据组和用户账号的设置规则，对该学校的各个部门所属的“域”进行规划，进一步划分“组”账号，并规定了组中的用户账号、密码以及各个“组”所隶属的域等。明细清单详见表 8-2。

③ 确定 NT 网络的账号、密码和权限清单。

在账号的管理中应注意使用“最小特权原则”，即在执行不同的任务时，仅使用能够完成该任务的具有最小特权的账号。例如：一个系统管理员应当有两个以上的账号，一个是 administrator，另一个是普通的 user，当他要进行系统维护工作时，就使用管理员身份登录；而当他进行一些日常操作时，则以普通用户（user）的身份登录就可以了，这样设置比较安全合理。

（3）系统目录权限的规划

在上述规划完成之后，还应当对网络系统的共享资源进行合理的规划，例如，可以对服务器上的目录和文件资源进行合理的权限分配，从而达到资源优化的目的。参见表 8-3。

表 8-2 某校“单主域”模式的 NT 网络中“域”、“组”和用户账号明细清单

用户账号	密　码	部门或人员	使用者	系统默认权限分配	隶　属　组	隶　属　域
Adm GZH	Sxh12345	网络中心	郭正昊	ABCDEF GHIJK	Administrator	
Xming	Wh	网络中心系统维护人员	夏明	A	whwg	NETDOMAIN
Zhli	Soft	网络中心软件人员	章立	A	softwg	NETDOMAIN
Wjun	harware	网络中心硬件人员	王军	A	hardwg	NETDOMAIN
Hhua	Chxu	计算机系软件教师	黄华	A	rjwg	JSJDOMAIN
Lli	weiji	计算机系微机教师	李丽	A	pcwg	JSJDOMAIN
Mping	xinhao	信息系信号教师	毛屏	A	xhwg	XXDOMAIN
Zying	wluo	信息系网络教师	周颖	A	wlwg	XXDOMAIN
Chong	jsjkz	自动化系计算机控制教师	常红	A	jsjwg	ZDHDOMAIN
Liming	zdkz	自动化系自动控制教师	黎鸣	A	zdkzwg	ZDHDOMAIN
Yhua	Student31	本科学生	9831	A	9831wg	STUDOMAIN
Hli	Student38	专科学生	99438	A	99438wg	STUDOMAIN

表 8-3 某校 NT 网络中“NETDOMAIN”域中对“组”、用户的目录权限分配表

组　名	用户账号名称	共享资源名称	目录共享权限的分配
Whwg	Xming	C:\WINNT	完全控制
		C:\program	读取
softwg	Zhli	C:\WINNT	读取
		C:\program	完全控制
	Xming	E:\application	完全控制
	Zhli	D:\office\word	完全控制
		D:\VB	完全控制
	Wjun	D:\VC	完全控制
…			

注意：使用“组”(组账号)进行管理时，组中的所有用户账号都具有“组账号”分配的权限。例如，Xming 隶属于 Whwg“组账号”，因此，它就具有了该组对目录享有的权限。

总之，在上述几部分工作的基础之上，就可以实现网络系统组织和用户优化管理的目的，从而使得一个各自为政、杂乱无章、管理无序的系统，成为一个优化的、组织合理和集中管理的有序系统。

8.4 网络用户管理规划的实施

8.4.1 信任(委托)关系的建立与删除

如前所述,在 Windows NT 网络中,通过信任(委托)关系的建立,实现域与域之间的联接关系,并通过它实现用户账号的跨域通行确认。

1. 建立单向信任(委托)关系

我们称委托者为“信任域”(trusting domain),称受托者为“受托域”,即被信任域(trusted domain)。建立信任(委托)关系的步骤分为两个主要部分。

① 先到“受托域”(被信任域)登录,设置允许其他域信任此“受托域”的操作。

② 再到信任域登录,设置允许信任“受托域” 被信任域的操作。

应注意的是:信任关系的建立是按顺序进行的,必须先设置受托域,后设置信任域。因此,请按照上面的操作步骤进行,否则会花费很长时间才能建立起信任(委托)关系。

2. 建立单向信任(委托)关系的实例

(1) 实例要求

以 ZDH-JSJ 域信任 ZDHDOMAIN 域为例,建立他们之间的单向信任关系。

(2) 解题说明

其中,ZDH-JSJ 域为信任域,ZDHDOMAIN 域为“被信任域”,即“受托域”。

(3) 建立步骤

第 1 部分:在 ZDHDOMAIN 域中,设置 ZDH-JSJ 域信任(委托)ZDHDOMAIN 域的操作步骤如下:

① 在 ZDHDOMAIN 域内的 PDC 上(Windows NT Server),以具有系统管理员 administrator 身份的账号登录。

② 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项,激活如图 8-8 所示的“域用户管理器”窗口。

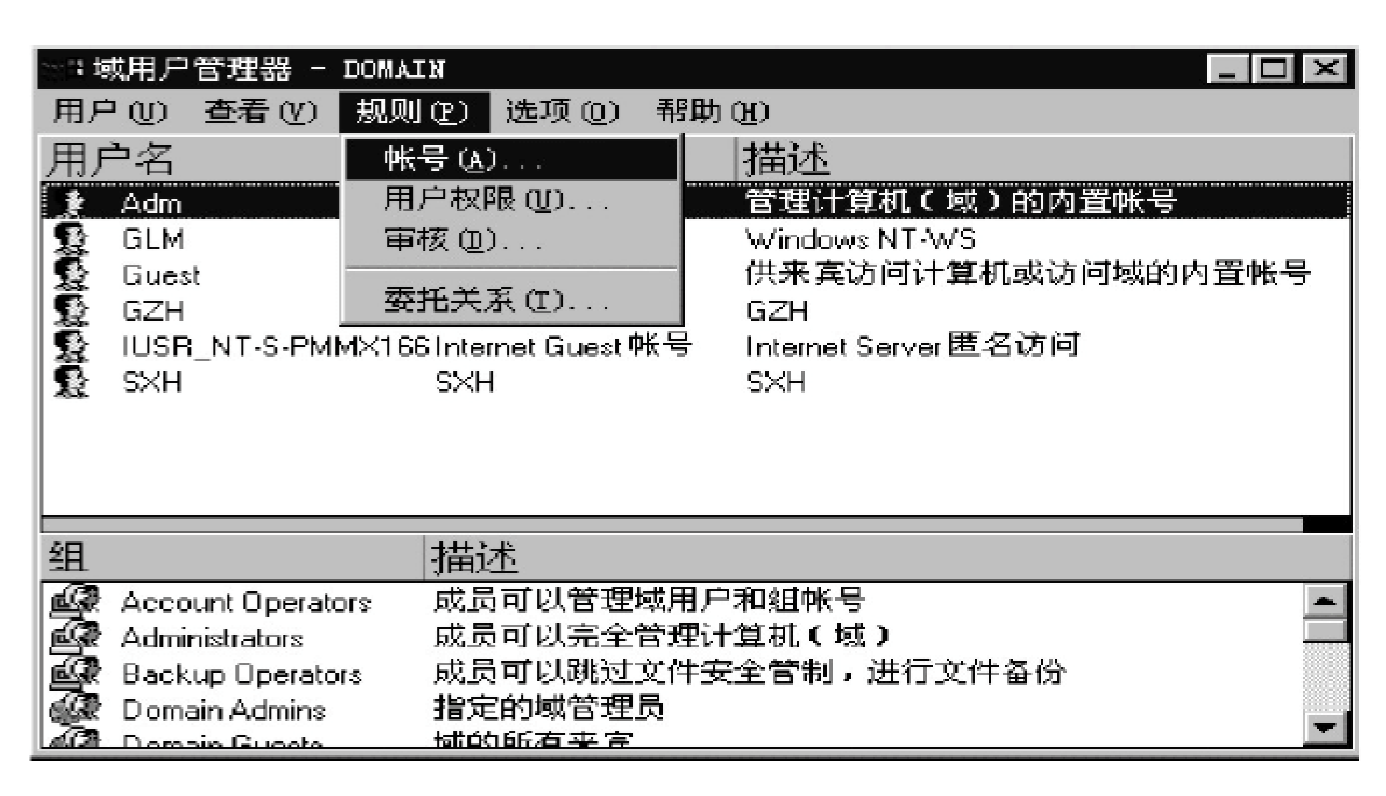


图 8-8 “域用户管理器”中的“规则(P)”下拉菜单

③ 在图 8-8 所示的窗口,选择“规则(P)”→“委托关系(T)”命令选项,激活如图 8-9

所示的“委托关系”窗口。

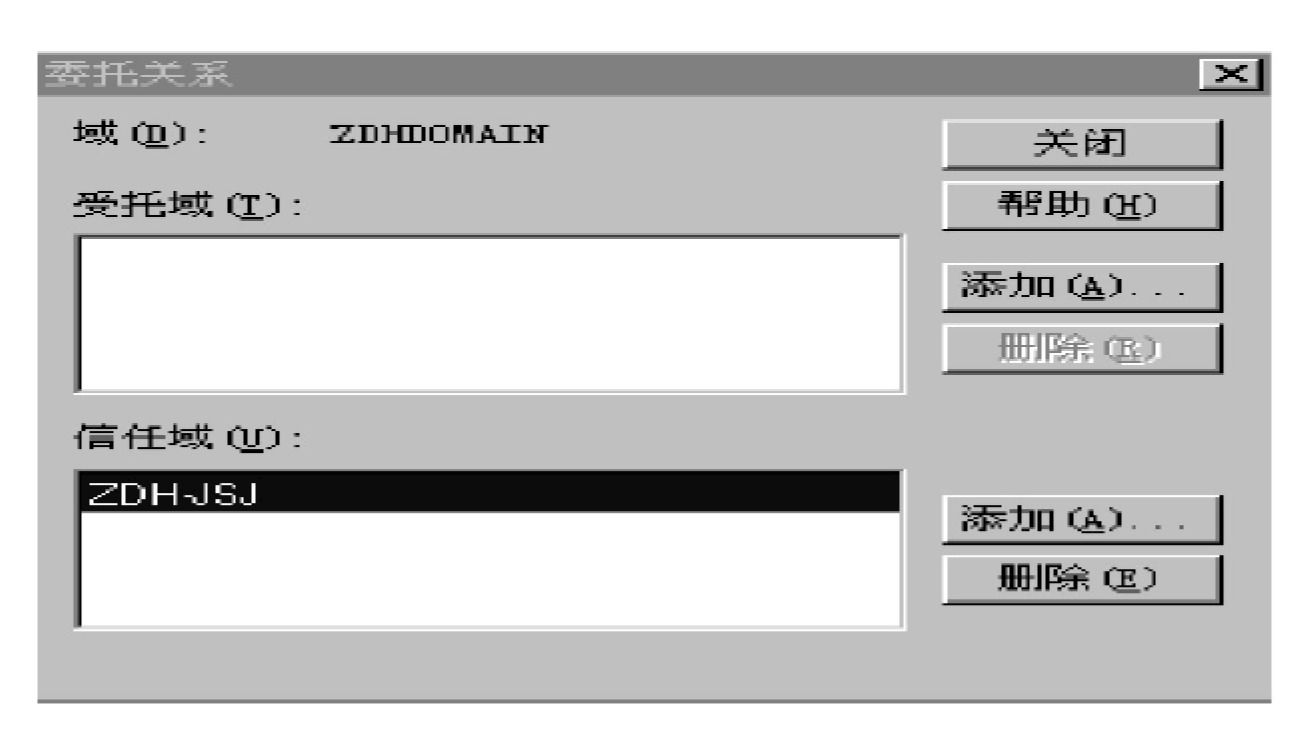


图 8-9 “审核规则”中的“委托关系”窗口

④ 在图 8-9 所示的窗口中,单击下方“信任域”右边的“添加”按钮,打开如图 8-10 所示的窗口。

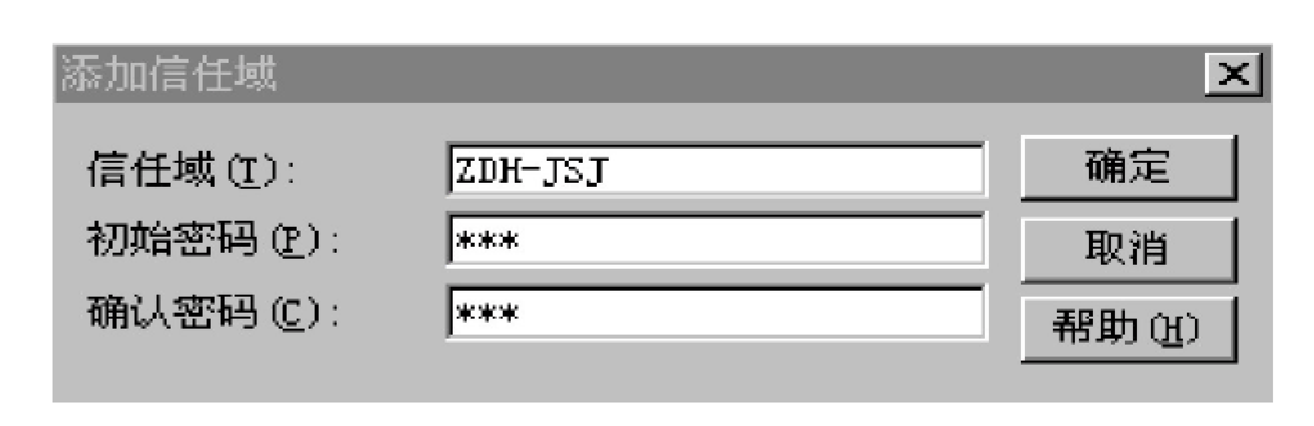


图 8-10 “委托关系”中的“添加信任域”窗口

⑤ 在图 8-10 所示的“添加信任域”窗口,设置允许 ZDH-JSJ 域可以信任 ZDHDOMAIN 域,同时输入密码。当 ZDH-JSJ 域的系统管理员在执行信任 ZDHDOMAIN 操作时,必须输入这个密码。单击“确定”按钮,完成。

⑥ 设置完成之后,在图 8-9 所示窗口的“信任域”列表中,将增加一个 ZDH-JSJ 域。

第 2 部分:在 ZDH-JSJ 域中,执行 ZDH-JSJ 域信任(委托)ZDHDOMAIN 域的操作如下:

① 在 ZDH-JSJ 域内的 Windows NT Server 上,以具有系统管理员 administrator 身份的账户登录。

② 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项,激活如图 8-8 所示的窗口。

③ 在图 8-8 所示的“域用户管理器”窗口,选择“规则(P)”→“委托关系(T)”命令选项,激活如图 8-9 窗口。

④ 在图 8-9 所示的“委托关系”窗口,单击窗口上方“受托域”(被信任域)右侧的”添加”按钮,打开如图 8-11 所示的窗口。

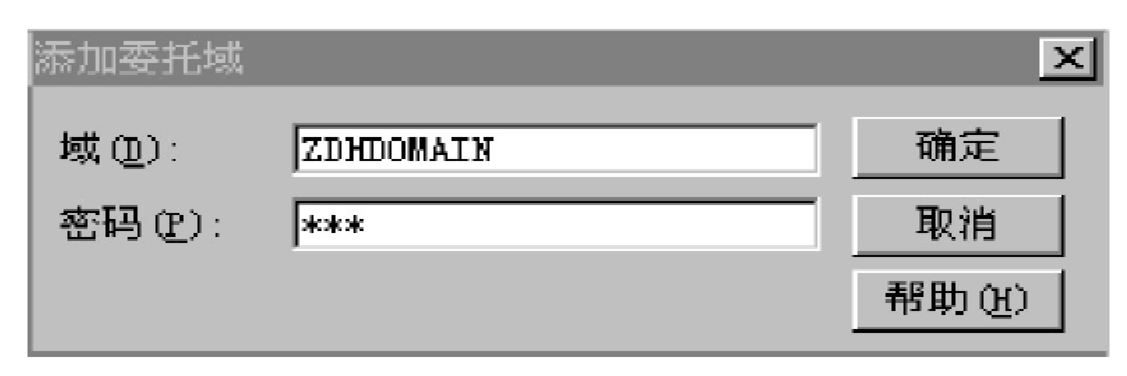


图 8-11 “委托关系”中的“添加受托域”窗口

⑤ 在图 8-11 所示的“添加受托域”窗口，输入 ZDH-JSJ 域需要委托的域名，即 ZDHDOMAIN 域。同时还须输入由 ZDHDOMAIN 域系统管理员设置过的密码。单击“确定”按钮，完成。

⑥ 设置完成之后，会出现“与 ZDHDOMAIN 的委托关系已创建成功的信息”，同时在图 8-9 所示的窗口的“受托域”列表中，将增加了一个 ZDHDOMAIN 域。

至此 ZDH-JSJ 对 ZDHDOMAIN 单向信任关系建立完毕。根据信任规则，ZDHDOMAIN 中的用户和全局组的成员就可以在 ZDH-JSJ 域中登录，并且拥有了以下权利：

- 在 ZDH-JSJ 域登录(logon)；
- 加入到 ZDH-JSJ 域的本地组(local group)中；
- 在 ZDH-JSJ 域中，可以访问被许可的资源，例如文件、打印机和其他共享资源。

3. 建立双向信任(委托)关系的实例

双向信任关系的建立是两个单向信任关系的组合。下面以 ZDH-JSJ 域和 ZDHDOMAIN 域为例，说明建立双向信任关系的过程。

① 一个单向信任关系是 ZDH-JSJ 域为信任域，ZDHDOMAIN 域为“受托域”(被信任域)。

② 另一个单向信任关系是 ZDHDOMAIN 域为信任域，ZDH-JSJ 域为“受托域”(被信任域)。

③ 双向信任(委托)关系的建立过程分如下两步：

- 建立 ZDH-JSJ 域信任(委托)ZDHDOMAIN 域的单向信任关系，过程与上述实例中建立单向信任关系的步骤完全一样。
- 建立 ZDHDOMAIN 域信任(委托)ZDH-JSJ 域的过程，可参照上述实例中的建立单向信任关系的步骤依次进行。

4. 信任(委托)关系的删除

删除信任关系时，用户应在信任域与被信任域(受托域)两端分别执行删除操作。删除操作的界面、工具与步骤简述如下：

① 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项，激活如图 8-8 所示的窗口。

② 在图 8-8 所示的“域用户管理器”窗口中，选择“规则(P)”→“委托关系(T)”命令选项，激活如图 8-9 所示的“委托关系”窗口。

③ 在图 8-9 所示的“委托关系”窗口中单击其中的“删除”按钮。

注意：*作为网络系统管理员来说，应该按照如下步骤执行：*

- 请先停止“受托域”(被信任域)用户使用的“信任域”中的资源。
- 再到“受托域”(被信任域)中，从“信任域”列表中选中要删除的域，单击“删除”按钮。
- 最后到“信任域”中，从“受托域”(被信任域)列表中选中要删除的域，单击“删除”按钮。

8.4.2 NT网络用户账号的建立

在域的PDC主域控制器建好之后，每个网络用户登录上网之前，必须向管理员申请一个用于上网登录的用户账号(账户)。每当用户上网时，都必须先输入申请到的账号名和相应的密码。为此，在对网络用户管理时，必须对系统中的可用账号(内置账号)有所了解，因为，管理员正是利用这些“内置账号”来完成系统账号的起始建立工作。

1. Windows NT服务器(或工作站)中的内置用户账号

那些未经建立就存在的账号，被称之为“内置账号”(或自带账号)。在Windows NT服务器(或工作站)的软件安装完毕之后，系统中有以下两个内置账号可供使用。

(1) administrator(系统管理员)

administrator是系统管理员，如果安装的计算机软件是Windows NT Server，另外该计算机是“主域控制器”(PDC)，则利用他可以管理整个“域”。如果安装的计算机软件是Windows NT Workstation(工作站)，则使用他只能管理本机。无论是前者还是后者，在辖区内他都拥有最高的权限。用户可以用这个账号来管理Windows NT Server(或工作站)上的资源，以及域(或本机)的账号数据库。如果认为administrator难记，可以在“域用户管理器”中加以改变，例如改为adm等。

(2) guest

guest账号是供那些临时用户使用的“内置账号”(自带账号)，它只拥有少量的权限。首次使用该账号之前，应选择“管理工具(公用)→域用户管理器”命令选项，在打开的图8-8所示的窗口中，单击guest账号，激活该账号的属性窗口。在该窗口中，将默认值选中的“账号暂时禁用”复选项取消。之后，对于那些很少使用网络资源的用户或网络来宾，就可以让他以guest账户身份登录NT网络。

2. 建立(添加)用户账号

实现添加用户账号的方法有以下两种。

其一，利用“管理向导”，选择“开始”→“程序(P)”→“管理工具(公用)”→“管理向导”命令选项，激活“管理向导”窗口，在该窗口单击“添加用户账号”按钮，添加新用户。

其二，使用“管理工具(公用)”中的“域用户管理器”添加用户账号。

下面仅介绍第2种方法。使用“域用户管理器”添加的用户账号的操作步骤如下：

① 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项，打开如图8-8所示的“域用户管理器”窗口。

② 在图8-8所示的“域用户管理器”窗口中，选择“用户(U)”→“新用户(U)”命令选项，在激活的“新用户”窗口中，应输入用户一些基本和必要的信息。建立用户账号时可按规划内容一次输入全部有关信息；也可以只输入用户的一些基本和必要的信息，其他内容则可根据用户的需要，在日后进行补充或修改设置。该窗口有关的信息如下：

ⓐ 基本用户信息　包括用户账号、全名、账号描述和密码等信息。用户的账号名称不能超过20个字节，另外，诸如“/ \ [ ] : ; | = . + ( )”等特殊字符不能在账号名称中使用。用户的密码不能超过14个字节，但没有不能使用上述特殊字符的限制。

ⓑ 组　用于设置用户所隶属的组，每一个用户账号可以成为多个组的成员。通过组

的设置,可以将性质相同的用户组织到一起,从而方便了系统管理。

ⓒ 配置文件　用来设置登录界面、登录启动程序和用户的宿主目录。

ⓓ 时数　用来设置允许用户登录网络的时间范围。

ⓔ 登录到　用来限定该计算机账号所能登录的域中的计算机站点。

ⓕ 账号　设置该用户账号的使用期限和账号类型。

ⓖ 拨入　设置该用户远程登录时的拨号权限和返回的参数。

③ 输入所要输入的信息后,单击“添加”按钮,完成建立账号的工作。

④ 如果打算将该用户加入组内,可先不按“添加”按钮,而单击“组(G)”按钮,激活“组员身份”窗口,从该图右部的“不隶属于(N)”中选择打算加入的组名,例如workgroup,然后单击“添加”按钮,完成加入组的工作。

⑤ 在加入选定的组之后,单击“添加”按钮,返回“新用户”窗口;最后单击“添加”按钮,完成建立用户账号和加入组的工作。

8.4.3 管理用户账号

1. 用户账户管理的主要内容

所谓管理用户账号是指以下几个方面的内容:

① 根据组的规划设计原则,建立用于管理的组。

② 建立和管理用户账号。例如,建立账号或账户模板,然后根据需要,对账号进行复制、修改或删除等项工作。

③ 设置账户的各种策略。

④ 给本地组设置资源访问权限。

⑤ 根据需要将全局组加入本地组。

⑥ 维护域控制器。

⑦ 排除登录故障。

2. 管理用户账户的有效方法

管理员为了完成每天的管理任务,保证网络通畅和正常运行,通常需要使用下面一些工作方法和工具,它们可以使得网络管理员的工作变得更加有效、快捷。

① 创建用户模板。使用用户模板可以迅速创建多个新的用户账号。

② 一次改变多个用户账号的属性。

③ 为了保证网络安全,设计和实现相应的账户策略。

④ 维护域控制器。使得用户账户总能被验证成功。

⑤ 解决用户账户登录时遇到的主要问题。

⑥ 通过创建 administrators 组,来完成网络的维护、管理安全等任务。

要完成上述任务,登录时用户的身份应当是 administrators、account operators 和 server operators 等组中的成员。

3. 创建用户模板和复制用户账户

如果网络上拥有许多性质相同的账号,可先建立一个用户模板,再使用复制账号的功能复制和建立这些账号。

账户模板复制时可以自动复制的项目：描述、组关系、可登录的时间、允许登录的工作站、账号有效期限与账号类型、“用户下次登录时必须更改密码”、“用户不得更改密码”、“密码永久有效”、“配置文件”和“拨入”等。

账户副本中用户必须新输入的项目：“用户名”、“全称”、“密码”和“确认密码”等。

实例　自动化系有 50 名教师，他们都隶属于 ZDH-T-GP 组，如果为每一位教师建立一个账号，并将他们一一加入到组中，显然会耗费很多时间。采用复制模板账号的功能的步骤如下：

① 先建立一个模板账号，例如 SXH，并将它加入到 ZDH-T-GP 组中。

② 在图 8-8 所示的“域用户管理器”窗口中，先选择复制对象，即模板账户 SXH，再选择用户(U)”→“复制(C)”命令选项，激活如图 8-12 所示的窗口。



图 8-12　拟复制账号“SXH 的副本”窗口

③ 在图 8-12 所示的“SXH 的副本”窗口中，必须输入账号中所有不能自动复制的项目，例如新账号的用户名、全称和密码等项目。

④ 在图 8-12 所示的窗口中，单击“添加”按钮，完成一个账户的复制工作。

⑤ 如此反复执行①～④，即可完成 50 个账号的建立工作。

由上可见，使用账号模板的复制功能建立多个具有相同类型的新账户，可节约大量时间。因此，在进行账户管理时，可以参照下列建议进行：

① 应当为每一个种类的账户建立一个模板。例如学校中的教师、管理人员和学生等。

② 如果需要管理一批使用性质相近的临时网络用户，也可以创建一个管理模板。例如，为登录时间、登录地点和其他的一些资源访问的限制条件相同或相似的用户创建一个模板。

③ 如果模板的“用户名”以一个非字母的字符开始，则这个账户模板总位于“域用户管理器”或“用户管理器”列表窗口的最上方。例如，用户名定义为：“_SXH”。

4. 修改用户账号

用户可以根据实际情况选择不同的方式。例如，修改用户账号时，可以每次修改一个或多个账号。

(1) 每次修改一个账号

第 1 种方法，在“域用户管理器”中，选择并双击要修改的账号。

第 2 种方法，选中某账号之后按 Enter 键。

第 3 种方法，在选中某账号之后，单击菜单项“用户(U)”，选择其中的“属性(P)”选项。以上 3 种方法都可以激活所选用户的“用户属性”窗口，修改后按“确定”按钮，完成修改工作。

(2) 每次修改多个账号

如果网络上拥有许多性质相同的账号需要修改某一参数，可使用多用户的修改方式。

① 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项，激活如图 8-8 所示的窗口。

② 在图 8-8 所示的“域用户管理器”窗口中选择账号的操作步骤如下：

- 按住 Ctrl 键，使用鼠标左键选取拟修改的不连续账号；
- 按住 Shift 键，使用鼠标左键选取拟修改的连续账号；
- 按住 Shift 键，使用上下箭头键选取拟修改的连续账号。

③ 在选中账号之后，选择“用户(U)”→“属性(P)”命令选项，激活如图 8-13 所示的多个账户的“用户属性”窗口，修改属性之后，单击“确定”按钮，完成修改工作。



图 8-13　多个账户的“用户属性”窗口

5. 删除用户账号

删除用户账号时，可以每次删除一个账号或多个账号。用户可根据实际情况选择不同的方式。在如图 8-8 所示的“域用户管理器”窗口中的操作步骤如下：

① 选择欲删除的账号。其方法如下所述：

- 按住 Ctrl 键，使用鼠标左键选取拟修改的不连续账号。
- 按住 Shift 键，使用鼠标左键选取拟修改的连续账号。

• 按住 Shift 键,使用上下箭头键选取拟修改的连续账号。

② 选中之后,单击菜单项“用户(U)”,打开下拉菜单条,选择其中的“删除(D)”选项,或按键盘的 Delete 键,激活确认窗口,确认之后完成删除账号的工作。

8.4.4 建立和管理组账号

利用“组”管理用户账号时,需要使用到“组账号”的概念。所谓“组账号”就是包含组中所有成员用户的账号。使用组账号可以方便和简化管理。赋予组的权限和许可时,对于组中的所有成员都会生效。在设计、规划好组账号之后,主要的工作就是如何创建需要的组,并根据规划将全局组加入合适的本地组中。

1. “组”的分类

(1) NT 中“组”的类型

NT 中的“组”可以分为全局组、本地组和特殊组。

① 全局组(global group)是由本域的域用户组成的,它是面向域用户的。它之所以被称为全局组,是因为全局组不仅能够在创建它的计算机上使用,而且还能在域中的任何一台计算机上使用,并且还能在跨域中(在信任域中)使用。但应注意,全局组中不能包含其他本地组和全局组。

② 本地组(local group)的“本地”指的是该组仅局限于所在的计算机和目录数据库,组中的成员是在一个目录数据库中定义的,并且可以赋予对其资源的访问许可。在一般的 NT 工作站和 NT 服务器上创建的本地组仅能在这台计算机上使用。而在 PDC 和 BDC 上创建的本地组,能在该域中所有的域控制器上使用。

③ 特殊组(especial group),NT 中还包含以下 4 个特殊的系统组:network 组、interactive 组、everyone 组和 greater owner 组。

(2) 全局组和本地组的比较

全局组和本地组的比较参见表 8-4。

表 8-4 全局组和本地组的比较表

比较项目	全 局 组	本 地 组
作用	用来组织域用户。全局组不仅能够在创建它的计算机上使用,而且还能在域中的任何一台计算机上使用,并且还能在跨域中(在信任域中)使用	用来给用户提供访问网络资源和执行系统任务的权限
组成	只能包含自己域的用户账户,不能包括本地组和其他全局组	经信任关系的建立,可包含任何域的用户账号和全局组。但不能包含任何其他本地组
创建位置与分配资源	总是在域中的 PDC 上创建,不被分配本地资源。一般用来组织和管理账号	在一般的 NT 工作站和 NT 服务器上创建的本地组仅能在这台计算机上使用。而在 PDC 和 BDC 上创建的本地组,能在该域中的所有域控制器上使用,如,分配资源,或赋予权限

（3）内置组

那些未经建立就存在的组，被称之为“内置组”。在 Windows NT 服务器（或工作站）的软件安装完毕之后，系统中有以下几种内置组可供使用：

① 内置的本地组。

- 内置本地组给予用户执行系统任务的权限。例如，该组的用户具有改变系统时间、备份/恢复文件，以及管理系统资源等权限。
- 所有运行 Windows NT 的计算机都有内置组。
- 内置组类别和具有的操作能力如下：

NT 计算机上具有的内置组的类型和各组具有的操作能力见表 8-5。

表 8-5　Windows NT 计算机上内置本地组的类型与操作能力

本地组名称	操　作　能　力
users	可以执行已被授权的任务，访问被分配许可的资源
administrators	在本地计算机上可以执行所有的管理任务，如果所在计算机是域控制器，则其成员可以管理整个域
guests	可以执行已被授权的任务，访问被分配许可的资源。但是，Guests 组的成员不能对本地环境做永久性的修改
backup operators	可以使用 Windows NT 上的备份程序对 Windows NT 计算机进行备份和恢复
replicator	该组不用于管理，仅为目录服务使用

NT 域控制器计算机上具有的内置本地组的类型，以及各组具有的操作能力参见表 8-6。

表 8-6　Windows NT 域控制器计算机上内置组的类型与操作能力

本地组名称	操　作　能　力
account operators	可以创建、删除和修改用户、全局组和本地组的账号信息；但不能修改 administrators 组和 server operators 组
server operators	可以设置磁盘资源的共享、备份和恢复服务器
printer operators	可以设置和管理打印机

② 内置的全局组。

- 内置的全局组使得管理员可以非常方便地控制和管理域中所有的用户。
- 只有主域控制器上存在内置的全局组。
- 当计算机安装了 NT Server，而成为域控制器时，在域的目录数据库建立了以下 3 种全局组，参见表 8-7。默认的内置全局组没有被分配任何权限，而只有当它们加入到本地组之后或被分配了用户权限或许可之后，才获得权限。

③ 系统组。

系统组的成员不是由管理员指定和分配的，即其成员是动态变化的。Windows NT 计算机上系统组的类型、组成和能力的描述，参见表 8-8。

表 8-7　域控制器计算机上内置全局组的类型和组成

全局组名称	组　　成　　员
domain users	当域用户账户创建时会自动成为该组的成员；本地 users 组会自动加入该组；administrators 账户默认时，也是该组的成员
domain admins	该组会自动加入到 administrators 组；administrators 账户默认时，也是该组的成员。domain admins 组的成员可以执行本地计算机的管理任务
domain guests	该组会自动加入到 guests 组。guests 账户默认时，也是该组的成员

表 8-8　Windows NT 计算机上系统组的类型、组成和能力

系统组名称	组成员及其操作能力
everyone	该组包含了所有访问计算机的本地用户和远程用户；它还自动包含所有访问该计算机的用户，包含 network 组、interactive 组和 guest 组。everyone 组与 domain users 组不同的是，它还包括了由管理员在域中创建的用户账户。administrators 组的成员可以给该组分配许可和权限
greater owner	该组包括一个资源的所有者，以及获得了其资源所有权的用户。如果某个管理员组的成员获得了一个资源的所有权，则此资源的新主人就是该管理员组，但是，只有在 NTFS 分区上，这个组可以用来管理文件和文件夹的访问任务
network	该组包括所有正在从网络上其他计算机连到你的计算机的共享资源上的用户
interactive	该组自动包括了从本地登录到计算机上的用户，该组的成员通过计算机之间的交互登录来访问资源

- 系统组（也称为特殊组），系统可以使用系统组来组织用户。
- 管理员不能为系统组分配组员，其成员随着网络的活动自动生成。
- 成员的关系可以被修改。
- 所有运行 Windows NT 的计算机都有系统组。
- 系统组的类型见表 8-8，其中，最主要的为 everyone 组和 greater owner 组。

(4) 使用本地组和全局组进行管理的最佳策略

① 使用本地组和全局组的策略。

- 使用全局组组织用户。
- 给本地组分配许可。
- 将全局组加入本地组。

② 使用 domain users 全局组进行管理。

请使用 domain users 而不是 everyone 全局组进行管理。因为，前者包括了已经创建的域用户账户；而后者则包括了所有从网络上联接的账户。

③ 实现跨域实施管理的目标。

为了实现上述目标，使得 administrators 组能够在其他域内实现管理，请将 domain admins 全局组加入到打算管理的域中的计算机的本地 administrators 组中去。

④ 实现特定管理的目标。

如果某个内置组的权限符合特定管理的需要，则可将所使用的用户账户加入到该内

置组中。当然,也可以创建一个本地组,并分配合适的用户权限,使之满足要求。

⑤ 实施最小特权原则。

根据用户的任务的需要,将其账户加入到严格限制的具有最低权限的内置组中去。

2. 使用“组”实施管理

(1) 创建“组”的规则

在创建和管理组账号之前,必须使用具有一定权限的账号登录。此外,创建的位置也是影响因素之一。总之,在创建“全局组”和“本地组”时应遵循如下规定:

① 登录账号必须是 administrators 组和 account operatortors 组的成员,或者是具有同等权限的用户账号。

② 可以在任何 Windows NT 计算机上创建本地组。

③ 通常在 PDC 上创建全局组,但是也可以在下列运行“域用户管理器”的计算机上创建。例如 BDC、域中的成员服务器及安装和运行 NT Server 管理工具的 NT Workstation 或其他 Windows 95/98/2000 计算机。

④ 在域中组的名称必须惟一,不得与其他用户的账号名或组名相同。

(2) 新建全局组

使用“管理工具(公用)”中的“域用户管理器”可以建立全局组,其步骤如下:

① 在图 8-8 所示的“域用户管理器”窗口中,选择“用户(U)”→“新全局组(G)”命令选项,激活如图 8-14 所示的窗口。



图 8-14 “新全局组”窗口

② 在图 8-14 所示的“新全局组”窗口中,键入“组名(G)”信息和描述(D)两项有关信息。

③ 在图 8-14 所示的“新全局组”窗口中,添加该组成员。先在右边“非成员”窗口选择拟加入该组的成员名单。然后,单击中间的“添加”按钮,即可将选中的用户加入至该全局组中。

④ 若想“删除”该组某成员,可在左边的“成员”窗口,选择拟删除的该组的成员名单。然后,单击中间的“删除”按钮,即可将选中的用户从该全局组中删除。

⑤ 最后,单击“确定”按钮,完成全局组的建立工作。

(3) 新建本地组

使用“管理工具(公用)”中的“域用户管理器”添加组账号和建立本地组的方法与建立

全局组时类似。用户可以参照前面的步骤进行。

（4）删除组

删除组的操作仅仅是删除了该组的名称、有关描述和与其关联的权限许可，而并未删除该组包含的所有用户账号。删除组的操作步骤如下：

① 在 NT Server 启动如图 8-8 所示的“域用户管理器”窗口，或者在 NT Workstation 中启动“用户管理器”。

② 选择拟删除的组名。

③ 按键盘的 Delete 键，或者在图 8-8 中选择菜单命令“用户（U）”，激活下拉菜单，从中选择“删除”选项，均可完成删除组的操作。

8.5 用户工作环境的管理

8.5.1 用户环境配置文件

1. 用户环境配置文件的作用

用户环境配置文件就是 profile 文件。它是为用户登录环境所配置的文件，在用户的基础上它存储每台 NT 计算机上的环境配置信息。它的主要作用是配置用户的工作环境。其内容包括桌面布局、个人程序组、程序项、屏幕色彩、屏幕保护、网络联接、打印机连接和鼠标设置等，这对于建立一个结构化的网络环境是非常有用的。当安全性需要绝对或部分控制时，或者用户不能对自身的工作环境来配置时，使用 profile 文件也是必要的。

2. 用户环境配置文件（profile）的分类

用户环境配置文件（简称环境文件，或 profile 文件）共有 4 种类型。

① 系统默认的 profile 文件　主要用于配置显示器（色彩和壁纸），直到有用户使用该计算机。

② 用户默认 profile 文件　如果没有给一个用户指定一个基于服务器的 profile 文件，那么该用户第一次使用计算机时，默认桌面设置将被拷贝到本地的用户环境配置文件，成为用户默认的用户环境配置文件。

③ 本地的 profile 文件　本地的 profile 文件主要用于在工作组的模式下。如前所述，如果计算机的管理员没有给某用户指定一个 profile 文件，则当这个用户第一次使用计算机时，将调用用户默认的 profile 文件。此用户默认将会在本地存储和命名，并且成为该用户的本地 profile 文件，该文件只能在本地使用。

在工作组模式下，用户使用本地的 profile 文件，如果一个用户到另一个计算机上登录，那么，他看到的将不是原来所熟悉的工作环境，他必须再次对环境进行配置。

④ 基于服务器的 profile 文件　基于服务器的 profile 文件是采用登录环境文件编辑器而建立的登录环境文件，它存储在服务器上，可以控制其他工作站上的用户桌面配置，主要用于域的模式下。域的管理员可以给一个域用户指定一个基于服务器的 profile 文件。于是这个域用户不论从域中的哪台计算机上登录，都将从服务器上调用同一个 profile 文件，而对工作环境所作的任何改变也将保存到服务器上。

基于服务器的 profile 文件类型又分为两种，即个人(.usr)和强制性(.man)环境文件。一个用户的环境配置文件，可以有一个“强制性”的环境文件，或者有一个“个人”的环境文件，但不可以两者兼而有之。

- 个人登录环境文件(.usr)　它实现部分控制，可以为每个用户提供单独的设置。
- 强制性的登录环境文件(.man)　它实现绝对控制，可以为一批用户提供共同的设置。

3. 用户环境配置文件(profile)的应用实例

(1) 环境配置文件实例要求

① 将某用户(例如 administrator)账号的环境参数设置给其他网络上的用户使用。使得这个域用户，无论从域中的哪台计算机上登录，都可以从服务器上调用同一个环境配置(profile)文件(即得到同样的工作环境)。

② 当此域用户登录后对环境所作的修改将保存到服务器上。

(2) 设置环境配置文件的步骤

① 依次选择“开始”→“程序(P)”→“Windows NT 资源管理器”命令选项，在打开的资源管理器窗口中，定位到“Winnt\Profiles\Administrator”，使其成为共享，其权限设置为“everyone→完全控制”。

② 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”命令选项，激活如图 8-8 图所示的窗口。

③ 在图 8-8 所示的“域用户管理器”窗口中，双击需要使用 administrator 账号环境参数的用户(例如 SXH)，打开该用户的“用户属性”窗口，单击其中的“配置文件(R)”按钮，激活如图 8-15 的窗口。

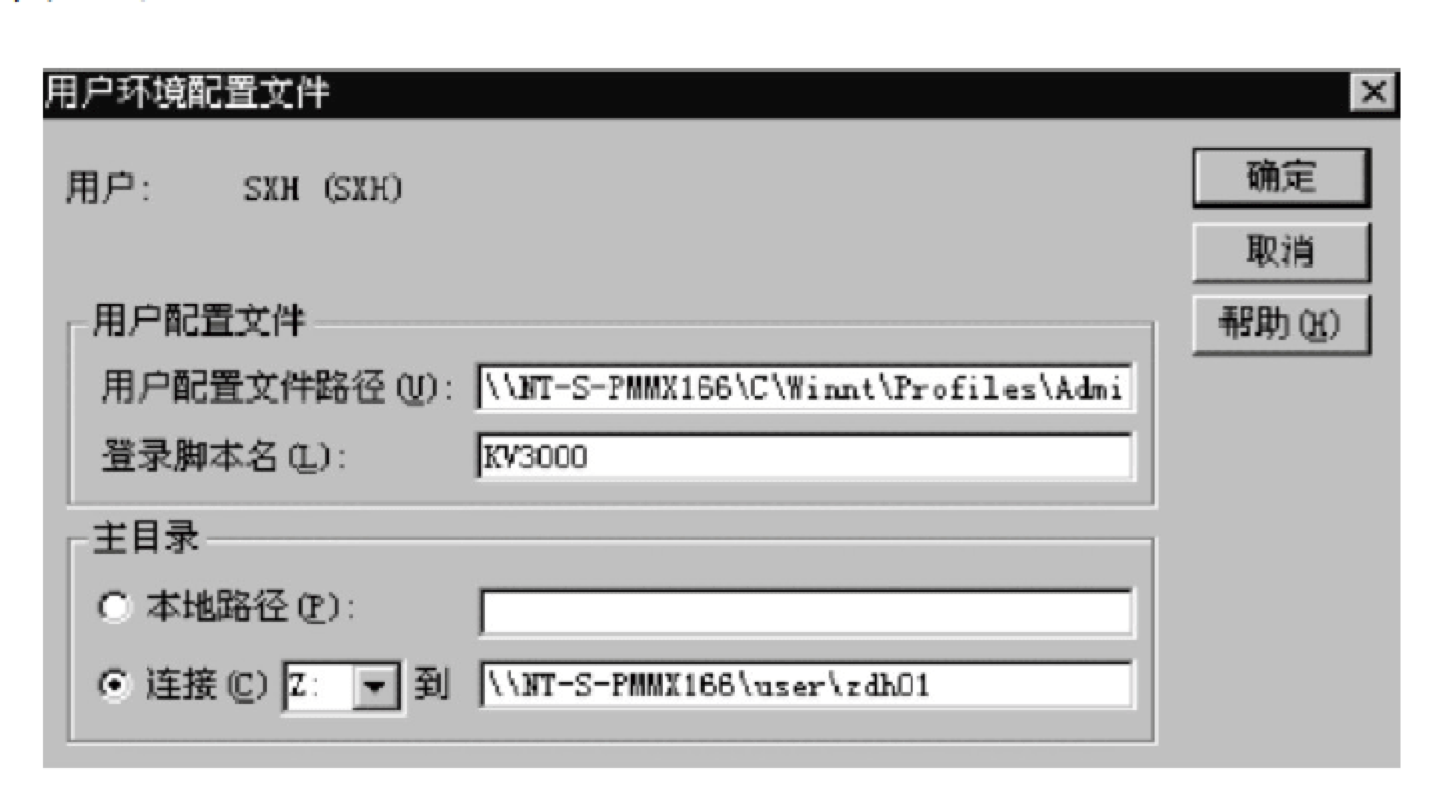


图 8-15　“用户环境配置”窗口

④ 在图 8-15 所示的窗口中的“用户配置文件路径”框内，键入引用环境文件的路径，此处应为“\\NT-S-PMMX166\C\Winnt\Profiles\Administrator”。

⑤ 单击“确定”按钮，完成设置。

⑥ 再次启动时，可以发现，使用“SXH”账号登录时的界面环境与使用 administrator 登录时的一样。

8.5.2 登录底稿

登录底稿(logon script),也被称为登录脚本。它通常是一个批处理文件或命令文件(.bat 或.cmd),其中包含了 DOS、OS/2 命令,或其他可执行文件。登录底稿和 profile 文件一样,也是用于配置用户工作环境的文件。实际上使用 profile 文件就能够实现登录底稿所能做的所有事,那么为什么还要采用登录底稿呢?其主要原因如下:

① 当用户从 DOS 或 OS/2 工作站上登录时可采用登录底稿;

② 能更方便地管理网络连接;

③ 易于升级已使用登录底稿的 LAN manager 网络。

实例　实现某用户(如 SXH 账号)登录成功之后,将自动执行某一批处理文件,或某一命令文件。例如:使用 SXH 账号登录后,首先启动一个杀毒工具 KV3000,该程序的路径为“E:\KV3000\KV3000.EXE”。

解:

① 使用编辑器编写的 KV3000.bat 文件内容如下

```
E:
cd \KV3000
kv3000
```

② 将 KV3000.bat 文件保存在计算机名称为“NT-S-PMMX166”的服务器的目录下,该文件的目录路径为“\winnt\system32\Repl\import\script”。

③ 将上述文件设为共享,共享名为 KV3000。

④ 在图 8-15 中的“登录脚本名(L)”文本框中,键入批处理文件的共享名 KV3000。

⑤ 当该用户再次注册登录时,便会自动执行此批处理文件。

8.5.3 宿主目录

1. **宿主目录**(home directory)

宿主目录也叫私有目录,该目录使得用户有一个固定的地方可以存储个人的程序和数据文件,从而使硬盘的管理更加方便。宿主目录由管理员为用户指定,它可以在本地硬盘,也可以存放到服务器上。设置之后,如果启动 DOS 命令指示符,则用户的默认路径为宿主目录。另外,如果某些应用程序没有指定工作目录,则打开和保存操作将在宿主目录下进行。

2. 本地路径

本地路径用来指定用户登录工作站的本地宿主目录的路径。例如 C:\SXH。

3. 共享网络目录

共享网络目录一般用网络驱动器进行连接。其中,“连接到”选项的作用是将某个网络驱动器与网络上的某个共享目录连接起来,并将它作为用户计算机的宿主目录。例如,可以在“连接”中指定网络驱动器 Z,再键入“\\NT-S-PMMX166\user\zdh01”。

4. 宿主目录实例

将服务器上的网络共享目录指定为某用户登录成功之后的宿主目录(例如 SXH 账

号的宿主目录)。设置的步骤如下:

① 在服务器上建立用户宿主目录:例如 C:\user\zdh01。

② 共享服务器上的 C:\user\zdh01 目录。

③ 打开如图 8-8 所示的“域用户管理器”中的某一用户,(例如 SXH)。打开该用户的“用户属性”窗口,单击其中的“配置文件(R)”按钮,激活如图 8-15 所示窗口。

④ 在图 8-15 所示的“用户环境配置”窗口,先选中“连接”单选钮。然后指定驱动器 Z 为网络驱动器,即使用盘符 Z 代表所指定的网络共享目录。在其后边的文本框中,输入指定的宿主目录名称,例如“\\NT-S-PMMX166\user\zdh01”。

⑤ 设置好宿主目录后,重新启动计算机,并以此用户名登录。启动后,依次选择“开始”→“程序(P)”→“DOS 命令提示符”命令,进入 DOS 环境,检查是否已将目录转入刚才指定的宿主目录。例如,应转入\\NT-S-PMMX166\user 上的“Z:\zdh01”目录下。

习题

1. 选择题

(1) 将一台计算机安装为 BDC,并且将其加入到 ZDHDOMAIN 域中,但是在安装过程中,错误地将其加入到了 DOMAIN 域中,如何解决这个问题?

A. 将这台计算机从 ZDHDOMAIN 域中迁移到 DOMAIN 域

B. 在 BDC 上的控制面板中的网络选项下,将域名变为 DOMAIN

C. 重新安装计算机,并将其加入到 ZDHDOMAIN 域中

D. 在登录时,选择 DOMAIN 域

(2) 如何将一台 Windows NT workstation 计算机加入到域中?(多选)

A. 在 Windows NT workstation 计算机上,从控制面板下的网络中改变域名,即可加入到域中。

B. 在 PDC 上为 Windows NT workstation 计算机创建一个计算机账号,再从 Windows NT workstation 上选择域名加入到域中。

C. 在 PDC 上为 Windows NT workstation 计算机创建一个计算机账号,它就自然加入到域中。

D. 在安装 NT workstation 时提供域名、域管理员的名字和口令,即可加入到域中。

(3) 有四个域甲、乙、丙、丁。甲信任乙,乙信任丙,丙信任丁,甲信任丙,乙信任丁,则在丁中创建的全局用户能访问哪些域中的资源?

A. 甲、乙、丙、丁

B. 乙、丙、丁

C. 丙、丁

D. 丁

(4) adm 是域 A 的管理员,如果他想同时管理 B,该如何实现?(多选)

A. adm 利用域用户管理器,使自己成为域 B 的管理员

B. 创建 A 信任 B 的关系
C. 创建 B 信任 A 的关系
D. 域 B 的管理员利用域用户管理器将 adm 加入到管理员本地组中
(5) 何时发生传递验证?(多选)
A. 当信任域的用户在被信任域中的某台计算机上登录时
B. 当被信任域的用户在信任域中的某台计算机上登录时
C. 当被信任域的用户访问信任域中的资源时
D. 当信任域的用户访问被信任域中的资源时

2. 问答题

(1) 域的目录数据库存放在什么位置?
(2) 域中的账户创建在什么位置?
(3) 目录服务的目标是什么? NT 网络是如何实现这个目标的?
(4) 什么是账号管理的集中?
(5) 什么是用户配置文件(user profile)? 它有什么用? 如何使用它?
(6) 什么是"域"的网络组织方式? 建立"域"有什么好处?
(7) 常用的"域"的组织模式有几种? 各适应于什么场合?
(8) 在"域"的模式下如何实现资源的互相访问?
(9) 什么是信任关系(trust relationships)? 为什么要使用信任关系?
(10) 什么是资源域? 什么是账户域? 何时发生传递验证?
(11) 什么用户环境? 用户环境设置包括哪几方面?
(12) 本地组和全局组用户的区别? 作用各是什么?
(13) 内置的本地组和内置的全局组的区别是什么?
(14) 实现本地组和全局组进行管理的最佳策略是什么?
(15) domain users 组和 everyone 组的区别是什么?
(16) 什么是用户的 profile 文件,它的作用如何?
(17) 什么是登录脚本? 它的作用如何?
(18) 什么是宿主目录? 用户可以使用的宿主目录有几种? 它们的作用如何?
(19) "工作组"和"组"有什么不同?
(20) "组"有什么用途? NT 中有哪几类组?
(21) Windows NT 网络的用户管理具体的内容有哪些?
(22) 请解释用户和用户账号的概念。
(23) 什么是建立账号的"最小特权原则"? 请举例说明,应当如何应用到网络的账号管理中?
(24) NT 网络组织的优化方法是什么? 在实际中应考虑哪些问题? 请以本单位的实际系统为例,写出应用的主要步骤。
(25) 如何使用"组账号"进行管理? 如何为组账号赋予某项权限? 写出主要步骤。

3. 应用题

(1) 对你单位的 Windows NT 网络用户进行优化管理,画出 NT 网络管理的目录

“树”，列出管理用的 NT 网络中“域”、“组” 和用户账号的明细清单。

（2）对你单位的 Windows NT 网络域中的共享目录的权限进行合理的划分。

实训题目

账号、组与域的建立与管理。

实训题 1

① 创建一个用户账号 Wang，它的描述信息为 Info studs。

② 设置“用户不得更改密码”有效。

③ 在创建账号 Wang 的同时，创建一个目录名为 Wang 的用户的宿主目录。

④ 设置用户 Wang 可登录到网络的时间为星期二至星期五上午 8：00～10：00。

实训题 2

① 按照实训题 1 中的内容创建模板账号“_Infostud”。

② 使用已创建的模板账号“_Infostud”分别创建 3 个用户账号 Info1、Info2 和 Info3。

③ 设置用户账号的规则：设置“密码最长期限为 30 天到期”、设置“最短密码长度为 7 个字符”、设置“最短密码期限为允许立即更改”和设置“登录 3 次失败后锁定账号”。

实训题 3

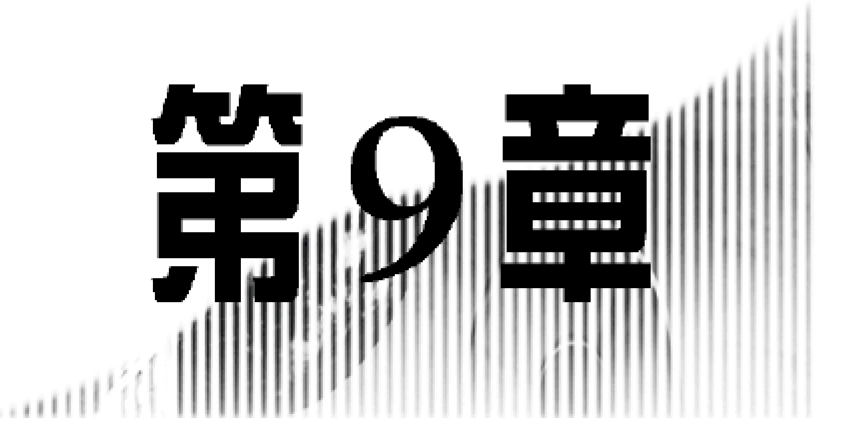
① 每 2 个学生一组，构建信任（委托）关系。建立单向信任。

② 要求受托域（资源域）中设置 1 个共享文件夹，其具有被信任域（账户域）中的 adiminstrators 组更改的共享权限。给信任域中的 local 组拒绝访问的权限，并在上述两个组中加入测试用户账户 atest 和 ltest 来验证共享效果。

实训题 4

① 按书中的学校部门分配情况建立起域的信任关系，建立一个主域和多个部门域。

② 建立主域与各信任域之间的单向信任关系。



第9章 网络中计算机和共享资源的管理

本章将介绍如何使用“服务器管理器”和其他系统工具管理计算机以及共享资源的基本概念和网络管理员应掌握的基本技能。

主要内容：

- NT Server 中的“服务器管理器”；
- 启动 NT“服务器管理器”；
- 使用“服务器管理器”选择和查看管理对象；
- 使用服务器管理器管理域中的计算机和用户；
- 与共享资源相关的概念；
- 创建和管理共享资源；
- 使用共享资源中的故障处理；
- 给某计算机上的已连接用户发送信息；
- 管理域；
- 控制面板内的服务器管理工具。

9.1 管理计算机和共享资源的基本工具

9.1.1 网络管理员在日常管理中的职责

在网络建成之后，网络管理员在日常管理工作中的职责就是对网络中的用户、计算机和共享资源进行管理。其中包括了多种类型的工作，主要的有以下几项：

① 在关闭主机或进行系统维护之前向各个用户或计算机发送信息。

② 监控和管理网络中共享资源的使用情况。

③ 对“域”或“工作组”中的计算机进行管理。

④ 管理和接收警报列表。

⑤ 管理网络用户的连接。

各种网络操作系统均提供了完成上述工作的工具。NT Server 中的“服务器管理器”就是 NT 网络中实现上述管理功能的主要工具之一，在 NT Workstation 中也有类似的工

具，但功能不及 NT Server 强大。

9.1.2 “服务器管理器”的功能

“服务器管理器”是用来管理域和计算机的工具窗口，使用它可以完成如下的功能和基本操作：

① 选择管理区域　可以选择要管理的域、工作组或计算机。

② 管理域中的计算机　其中包含查看选定计算机上的已连接用户列表、查看已共享和打开资源的使用情况、管理和目录复制、管理和接收警报列表、管理服务和共享目录，以及给已连接的用户发送信息等。

③ 管理域　其中包括将备份域升级到主域控制器、同步主域控制器和服务器，以及在域中添加或删除计算机等。

④ 管理域内共享资源。

⑤ 管理接收到的警报列表。

⑥ 管理服务。

⑦ 给某计算机上的已连接用户发送信息。

对于装有 NT Server 的计算机使用“服务器管理器”可以完成上述操作。每一台 Windows NT(工作站或服务器)的“控制面板”上的“服务”或“服务器”工具中，也包含有“服务器管理器”所提供的部分功能。但是，“服务器管理器”可以管理本地和远程计算机，而“控制面板”中的服务工具只能影响本地计算机。

9.1.3 使用“服务器管理器”的账号

在 NT Server 中使用“服务器管理器”管理域及其服务器时，必须以该域的 administrators、domain admins 或 server operators 组成员的用户账号登录。account operators 组的成员也可以使用“服务器管理器”，但是它只有将计算机添加到域的权限，没有其他权限。

必须以计算机的本机管理员，或该特权用户组的成员的用户账号登录，才能使用“服务器管理器”管理工作站的计算机，或管理运行 NT Server 的其他服务器(非主域控制器)。而“服务器管理器”的一些功能，则只允许由系统管理员或域管理员使用，当其他用户使用这些功能时，将遭到拒绝。

9.1.4 启动“服务器管理器”

启动 NT“服务器管理器”的步骤如下：

① 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“服务器管理器”命令选项，激活如图 9-1 所示的窗口。

在大部分情况下，当“服务器管理器”第一次启动时会显示所登录的域。“服务器管理器”标题栏上方会显示出“域名”，例如图中的 ZDHDOMAIN，并且在“服务器管理器”窗口中列出该域内的所有计算机。

② 管理员可以从图 9-1 所示的计算机列表窗口中，选择欲管理的计算机，然后，可以



图 9-1 “服务器管理器”窗口

使用“计算机”菜单中的各种命令对列出的计算机进行管理。

9.2 使用“服务器管理器”管理域中的计算机

服务器管理器的一个重要职责就是管理服务器，而系统管理员对服务器的管理是通过对服务器的属性进行设置来完成的。因此，可以说，管理服务器就是对服务器的属性进行查看、修改和删除等操作。

9.2.1 服务器管理器的属性窗口

1. 启动某计算机的属性窗口

选择并启动某服务器“属性”窗口的步骤如下：

① 在图 9-1 所示的窗口中，双击“服务器管理器”窗口中的服务器计算机名，激活如图 9-2 所示的“选定计算机的属性”窗口，该窗口可以显示连接到该计算机的会话、打开文件、文件锁定和打开已命名管道等使用状况的统计数据。



图 9-2 “选定计算机的属性”窗口

② 若要修改计算机说明，请在图 9-2 所示窗口的“说明”文本框中键入相应文字。

③ 若要管理该计算机的“属性”，请选择并单击窗口底部有关的属性按钮。该计算机的属性设置共有 5 个按钮选项，即“用户”、“共享”、“使用中”、“复制”，以及“警报”。

④ 单击图 9-2 所示“属性”窗口中的“确定”按钮，完成对选定计算机的“属性”设置和管理工作。

2. 选定计算机属性窗口信息

在图 9-2 所示的窗口中,可以了解到选定服务器(计算机)的如下详细信息:

(1) 窗口的使用摘要栏目说明

① 会话:指远程计算机与选定计算机的用户连接数目。

② 打开文件:指远程计算机与选定计算机连接用户所打开的文件数目。

③ 文件锁定:指远程计算机与选定计算机连接用户所锁定的文件数目。

④ 打开已命名管道:指已打开的命名管道数目。命名管道是进程间的一种通信机制,它可以让一个过程与本地或远程的另一个过程进行通信。

(2) 窗口下方各按钮的说明

① "用户":使用该按钮可以查看网络上连接到该计算机上的所有用户列表,以及每个用户所打开的共享资源列表,还可以选择并切断用户与服务器的连接。

② "共享":使用该按钮可以查看该服务器所提供的共享资源和资源访问的用户列表,还可以选择并切断用户与服务器的连接。

③ "使用中":使用该按钮可以提供该计算机当前被使用的资源列表,还可以关闭或打开某个或全部的资源。

④ "复制":该按钮可以提供目录的复制功能。它利用网络上某台服务器作为导出服务器,将需要复制的目录导入其他需要此目录的计算机(即导入计算机)中。这样,管理员就无需在每一台被管理的客户计算机上都创建一遍该目录。然而,系统管理员应当注意,运行 NT Server 的服务器才具有目录的导出和导入的功能,其他的 NT 计算机仅有导入的功能。因此,应当将需要复制的目录放在 NT Server 服务器上。

⑤ "警报":用于管理和查看管理警报发生时要通知的用户和计算机。

9.2.2 服务器管理器中的操作

1. 查看"用户会话"信息

(1) 查看连接到计算机的用户列表的操作步骤

① 在图 9-1 所示的"服务器管理器"窗口中,双击计算机名,例如 NT-S-PMMX166,激活如图 9-2 所示的窗口。

② 在图 9-2 所示的某计算机的属性窗口中,单击"用户(U)"按钮,激活如图 9-3 所示的"用户会话"窗口。在该图中的"用户会话"窗口中,出现"已连接的用户"、"计算机"、"打开"、"时间"、"空闲"及"来宾"等状态信息。另外,对于"已连接的用户"还摘要显示出与本机远程连接的用户数量。

③ 在图 9-3 所示的窗口中,若要查看某一用户所打开的资源,请在"已连接的用户"列表框中,选择欲查看用户的用户名,下方的"资源"窗口中将显示与该用户连接的共享资源、打开和时间显示等信息,同时列出该用户所连接的共享资源。

④ 在图 9-3 所示的窗口中,若要退出,请单击"关闭"按钮,返回图 9-2 所示的窗口,然后单击"属性"窗口中的"确定"按钮,完成此项操作。

(2) 断开与某一用户的连接

在图 9-3 所示的窗口中,在"已连接的用户"的列表框中,选定欲断开用户的用户名,

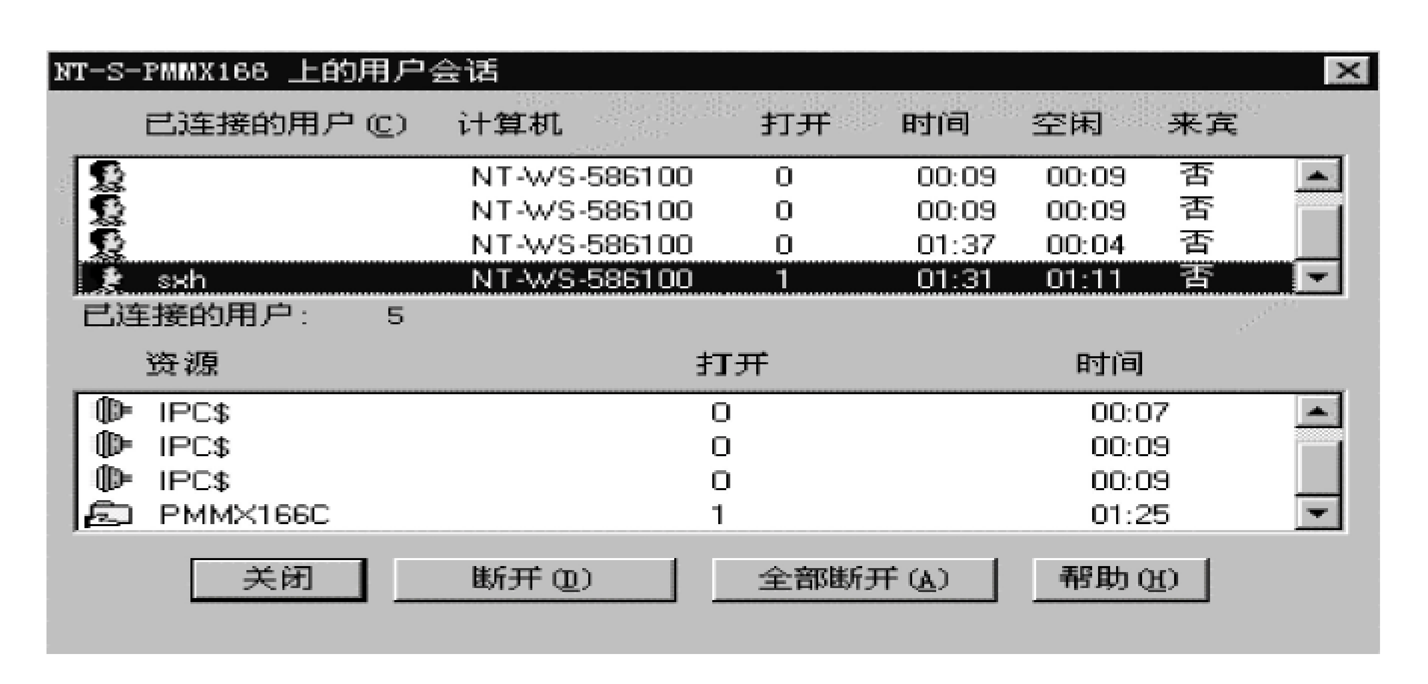


图 9-3 “选定计算机的用户会话”窗口

然后单击“断开”按钮。

（3）断开与所有用户的连接

系统管理员应该在断开服务器与所有用户的连接之前，告知已连接的所有用户，然后在图 9-3 所示的窗口中，单击“全部断开”按钮即可。

注意：当远程管理另一台计算机时，用户账号即被视为连接到 IPC＄ 资源列出，不能断开。IPC＄作为共享程序间通信所必备的命名管道资源，用于远程管理计算机和查看该计算机所使用的共享资源。

2. 查看和管理共享资源

（1）查看某计算机共享资源列表的操作

① 在图 9-1 所示的“服务器管理器”窗口中，双击计算机名，例如 NT-S-PMMX166，激活如图 9-2 所示的窗口。

② 在图 9-2 所示的“属性”窗口中，单击“共享”按钮，激活如图 9-4 所示的“共享资源”窗口。其中的“共享名(S)”窗口，列出了该计算机上所有可用的共享资源名、使用的用户数目和路径。

③ 若要查看连接到共享资源的用户，请在图 9-4 的“共享名(S)”窗口中选择一个共享名称，在该图的下半段的“已连接的用户”窗口中，将列出已连接的用户、时间及正在使用等信息。在“已连接的用户”栏目下，将摘要显示已连接的用户与选定资源连接的用户数量。



图 9-4 “选定计算机的共享资源”窗口

（2）管理某计算机共享资源列表的操作

① 要断开某一用户与所有共享资源的连接，请在图 9-4 所示的窗口中，选定“已连接的用户”窗口中的用户名，然后单击“断开”按钮。

② 要断开所有用户与所有共享资源的连接，请在图 9-4 所示的窗口中，单击“全部断开”按钮。

说明：按照管理的惯例，管理员在断开连接之前，应当提示已连接的用户，然后实施操作。断开连接之后，每一被断开连接的用户，将同时断开该计算机上使用的所有共享资源连接，而并非只断开在“共享名”选择框中所选定的资源。

③ 若要共享或管理共享目录，需要在图 9-1 所示的“服务器管理器”中，选择“计算机→共享目录”命令选项，或使用“Windows NT 资源管理器”在目录属性中设置共享及其属性。对打印机进行共享操作或管理共享的打印机时，请参阅第 11 章的内容。

注意：当远程管理另一台计算机时，用户账号即被视为连接到 IPC＄ 共享资源列出，不能断开。

(3) 查看和管理使用中的资源

查看计算机上使用中的资源的操作步骤如下：

① 在图 9-1 所示的“服务器管理器”窗口中，双击计算机名，例如 NT-S-PMMX166，激活如图 9-2 所示的窗口。

② 在图 9-2 所示的“属性”窗口中，单击“使用中(I)”按钮，激活如图 9-5 所示“打开资源”窗口。其中的“打开方式”窗口，列出了该计算机上所有已打开的资源。



图 9-5 “选定计算机的打开资源”窗口

③ 在图 9-5 所示的窗口中，单击“刷新(R)”按钮，可以更新显示信息。

④ 在图 9-5 所示的窗口中，单击“关闭”按钮，退出该窗口。

⑤ 在图 9-2 所示的“属性”窗口中，单击“确定”按钮，完成此操作。

(4) 管理计算机上使用中的资源的操作步骤

① 在图 9-5 所示的窗口中，先选定正被使用的资源，然后，单击“关闭资源(C)”按钮，可以关闭已打开的选定资源。

② 在图 9-5 所示的窗口中，单击“关闭所有资源”按钮，可以关闭所有被打开的资源。在关闭资源之前，管理员应当提示、警告与该资源连接的各用户。当远程管理另一台计算机时，用户账号即被视为连接到 IPC＄ 共享资源列出，不能关闭。

3. 使用系统管理警报

（1）使用系统管理警报的原因

当计算机发生故障时，例如，硬盘容量不足、打印机出现问题、或 UPS 检测到停电信息等，管理员可利用警报工具，让计算机自动发送警报信息给系统维护者，或将提示信息送到指定的计算机屏幕上。

（2）使用系统管理警报

发送警报信息的计算机应当启用 Alerter 与 Messenger，而接收信息的计算机必须经过一定的设置才能收到警报信息。设置步骤应根据工作站的不同而有所不同。

接收“管理警报”的计算机和用户的设置步骤如下所述：

① 在图 9-1 所示的“服务器管理器”窗口中，双击计算机名，例如：NT-S-PMMX166，激活如图 9-2 所示的窗口。

② 在图 9-2 所示的“属性”窗口中，单击“警报(A)”按钮，激活如图 9-6 所示的警报窗口。

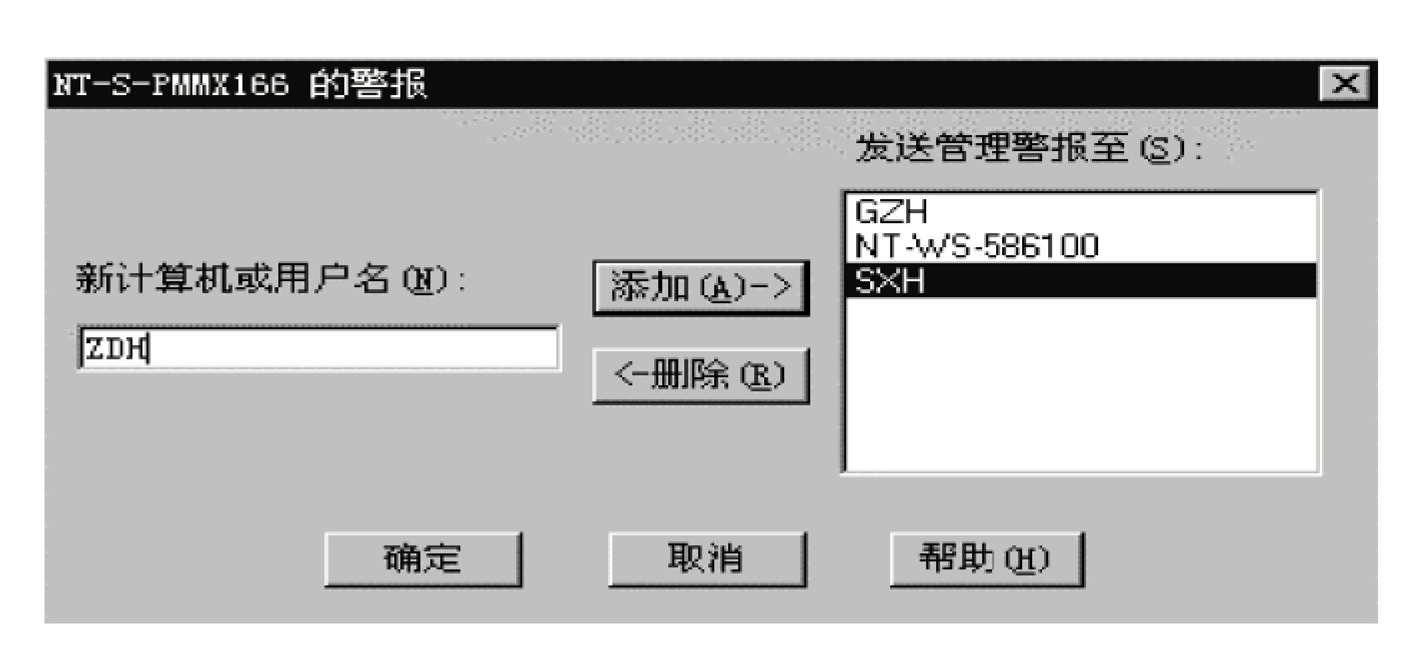


图 9-6　“选定计算机的警报”窗口

③ 在图 9-6 所示的窗口中，应将用户或计算机添加到警报接收方列表中，请在“新计算机或用户名”框中输入用户名或计算机名，然后单击“添加(A)”按钮。

④ 要从警报接收方列表中删除用户或计算机，请先选定“发送管理警报至”框中的用户名或计算机名，然后，单击“删除”按钮。

⑤ 在图 9-6 所示的窗口中，单击“确定”按钮，退出该窗口，返回图 9-2 所示的“属性”窗口。

⑥ 在图 9-2 所示的窗口中，单击“确定”按钮，完成设置。想使更改和设置生效，请终止并重新启动服务器管理器和警报服务。

注意：

- 可以先指定接收警报的计算机和用户，当发生管理警报时，系统就会通知已选定的计算机和用户；
- 管理警报由系统自动产生，并且和服务器及资源的使用有关，管理警报会自动警告安全性和访问问题、用户会话问题、打印机问题及使用 UPS 服务时由于断电导致服务器关机等问题。

9.3 管理共享资源

网络中所有应用程序和数据资料都是以目录和文件的形式存放在各种存储介质上的，一旦这些数据被损害将给企事业单位造成无可弥补的损失。因此，目录和文件的共享与管理是非常重要的日常管理工作。系统管理员一般通过管理共享文件夹（即目录）来保证网络资源的安全。

9.3.1 共享和共享目录的基本知识

1. **共享**（shared）

共享是 NT 的一个使用特点。通过设置共享来指定网络用户可以从网络上访问的资源。文件共享对于网络操作而言，是最基本和最重要的事情。例如：前面我们已经介绍过如何在 Windows 95/98/NT 中开放和使用共享资源。

2. 共享文件夹（shared folder）

共享文件夹又称共享目录（shared directory），通常用户通过它来访问网络上的应用程序、数据和用户的工作目录。当某目录设置为共享文件夹（目录）后，用户就可以集中地访问该文件夹中的所有文件。因此，作为系统管理员，在用户连接和使用共享目录之前，应当先对所要开放的文件和目录进行整理，继而指定共享文件夹的访问权限，最后开放该共享目录。在管理共享文件夹的过程中应当注意以下几点：

① 指定共享资源　应按照文件和目录的用途整理共享文件夹。例如：指定应用程序目录存放可以配置和升级的应用软件；指定数据文件目录存放用户需要访问的各种数据；指定用户的主目录，以便备份和管理用户的工作数据。

② 删除 everyone 组的完全控制权限　这是管理共享中的一个重要步骤。

③ 共享权限（许可）的分配　按照用户和组的需要配置共享文件夹的访问许可。例如：当某用户需要添加和删除文件时，就应当为该用户分配“更改”的访问许可。而当某用户只需要读某个目录中的文件时，可以仅分配给他“只读”的访问许可。

④ 共享权限（许可）的分配对象　共享文件夹的许可，可以分配给“用户”和“组”账户。Windows NT 服务器提供给用户的许可可以分配给用户账户，或者组账户，也可以同时分配给用户和组账户。

3. 共享文件和文件夹的许可（权限）类型

为了控制用户对共享文件夹的访问，保证网络共享资源的安全，必须为共享文件夹分配许可。共享文件和共享目录许可的类型有拒绝访问、读取、更改和完全控制等几种。共享许可的具体内容参见第 15 章。

9.3.2 查看和管理共享目录

1. **查看共享目录**

查看共享文件夹的操作步骤如下：

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机名。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“共享目录(D)”命令选项，在激活的“共享目录”窗口中，列出了该计算机的共享目录及每个共享目录的路径。在这个窗口中，可以使用下述的按钮进行管理。单击“关闭”按钮，退出共享目录窗口。

- “新建共享(N)”按钮　用于添加共享资源。
- “属性(P)”按钮　用于修改共享资源的属性。
- “停止共享(S)”按钮　用于停止资源的共享。

2. 管理共享目录

“服务器管理器”中的共享目录的管理功能包含：添加、修改和停止共享目录等项。

管理共享目录的操作步骤如下所述：

(1) 添加新的共享目录

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机名。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“共享目录(D)”命令选项。

③ 在激活的“共享目录”窗口中，单击“新建共享(N)”按钮。

④ 在激活的“新建共享”窗口中，应该输入共享名、路径和备注等信息。若需设置允许同时连接到共享目录的用户数量，请在“用户个数”栏目下，对“不限制”和“允许”两个单选按钮进行选择。如果选择了“允许”单选按钮，则应在“个用户”框中，输入指定的最大数量。若需要管理组和用户的权限级别，请在图中单击“权限”按钮。

⑤ 在激活的“通过共享访问的权限”窗口中，可以进行有关的设置。设置之后，单击“确定”按钮。

说明：在更改默认值之前，新的共享目录将给 everyone 提供“完全控制”的访问权限，因此，必须先删除这个访问权限，否则任何权限的设置都将无效。

(2) 修改共享目录

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机名。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“共享目录(D)”命令选项。

③ 在激活的“共享目录”窗口中，单击“属性(P)”按钮，激活“共享属性”窗口。若要更改路径或说明，在“路径”或“备注”后的文本框中键入新的文字。若需要设置允许同时连接到共享目录的用户数量，在“用户个数”栏目下，对“不限制”和“允许”两个单选按钮进行选择。如果选择了“允许”单选按钮，则应在“个用户”框中，选择或输入指定的最大数量。若需要管理组和用户的权限级别，在图中单击“权限”按钮。

④ 在激活的“通过共享访问的权限”窗口中，可以进行有关的设置。设置之后，单击“确定”按钮。

(3) 设置已存在共享目录的权限

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机名。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“共享目录(D)”命令选项。

③ 在激活的“共享目录”窗口中，单击“属性(P)”按钮，激活“共享属性”窗口。在该窗口中，单击“权限”按钮，激活如图 9-7 所示的窗口。

④ 通过图 9-7 所示的窗口可以更改下列设置选项：

- 要更改权限，从"名称"列表中选定欲修改的权限，然后从"访问类型"框中选定权限，例如，将 administrator 账号的权限改为"更改"。
- 可以将组或用户账号添加到共享目录的权限列表中，请选择"添加"按钮，并且在"添加用户及组"窗口中完成添加用户账号或组账号的操作。
- 要从共享目录的权限列表中删除组或用户账号，请在图 9-7 所示的窗口的"名称"列表框中，选定组或用户，然后，单击"删除"按钮，完成删除操作。

⑤ 在图 9-7 所示的窗口中，完成更改后，单击"确定"按钮关闭窗口。

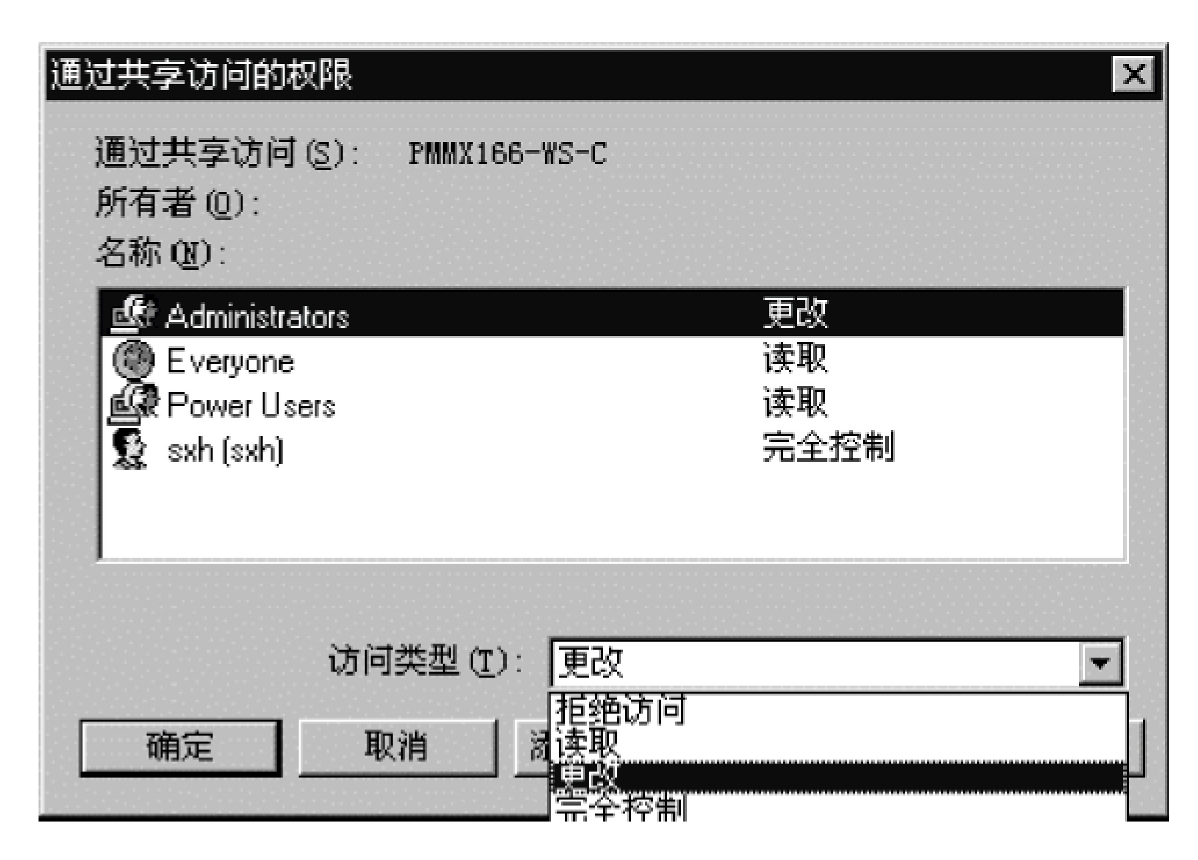


图 9-7 "通过共享访问的权限"窗口

提示：指定权限时，较好的方法是将权限指定给"组"账号，而不是指定给单个的"用户"账号。

(4) 停止已存在共享目录

① 在图 9-1 所示的"服务器管理器"窗口中，选定计算机名。

② 在图 9-1 所示的窗口中，依次选择"计算机"→"共享目录(D)"命令选项。

③ 在激活的"共享目录"窗口中，从列表中选定共享名，单击"停止共享(S)"按钮，完成操作。

注意：

- 目录本身并未删除，但是已不能再共享和被网络用户访问；
- 在大部分的情况下，不应该选定出现在列表中的由系统创建的特殊共享的共享名，例如 A＄、B＄、C＄、ADMIN＄、IPC＄、NETLOGON、PRINT＄ 或 REPL＄ 等项目。

3. 排除使用网络共享资源中的故障

排除使用网络共享资源中的故障是网络管理员的日常工作之一，也是最常见的问题。下面分别介绍网络管理员经常遇到的问题及其解决方法。

(1) 用户不能访问共享资源

检查分配给该用户账号和该用户账号所在的成员组的权限(许可)是否为"no access

(拒绝访问)”许可。因为,具有此类许可的账户就不能访问资源。

(2) 删除了某个具有“no access(拒绝访问)”许可的共享文件

有时,某个共享文件的所有者(用户)已经为文件分配了“no access(拒绝访问)”的许可,但是该文件还是被删除了。这种情况的发生,是由于该文件所在的文件夹被分配了“full control(完全控制)”的许可。因此,管理员在设置文件夹的共享权限时,一定注意将NTFS系统中默认的“full control(完全控制)”共享权限,改变为其他类型的访问许可。因为,一旦共享文件夹具有了“完全控制”权限,用户就获得了对该文件夹中全部文件的所有权限。

(3) 改变权限后尚未生效将导致用户无法访问指定了权限的共享资源

系统管理员已将某个用户加入到一个组中,并使他具有了访问某个共享资源的权限,但这个用户未能如愿以偿。这是因为,改变了权限的共享资源的许可尚未生效。此时,应当先让用户退出登录,然后再次登录注册;或者让用户先断开连接,然后,再次连接。

9.4 在各种计算机上发送信息

网络管理员经常需要向网络中的用户发送提示、警告或通知等信息,本节将介绍与此相关的技巧。

9.4.1 给某计算机上的已连接用户发送信息

① 在图9-1所示的“服务器管理器”窗口中,从计算机列表中选定计算机。例如:如果要给连接到某主域控制器上的所有用户发送消息,则应选择这个域的主域控制器“NT-S-PMMX166”。

② 在图9-1所示的窗口中,依次选择“计算机”→“发送消息(M)”命令选项。

③ 在激活的“发送消息”窗口中,先在“消息”文本框中输入消息的内容,然后单击“确定”按钮。

④ 操作完成后,会把此信息发送给所有与“NT-S-PMMX166”相连的用户,与之连接的用户将收到这则消息。

注意: *只有启动message功能的计算机才会收到传递来的信息,而不同的操作系统启动message功能的方法也有所不同。*

9.4.2 启动和使用计算机上的message(信使)功能

1. **启动NT Workstation或NT Server计算机上的信使(message)功能**

① 依次选择“开始”→“设置(S)”→“控制面板(C)”命令选项,在弹出的窗口中单击“服务”图标,激活如图9-8所示的窗口。

② 在图9-8所示的窗口中,选择Messenger,单击“启动(R)”按钮。

③ 在激活的“服务Messager”窗口中,在“启动类型”栏目下可以设置Messenger的启动方式。例如,选择“自动”单选项,然后,单击“确定”按钮,完成操作。

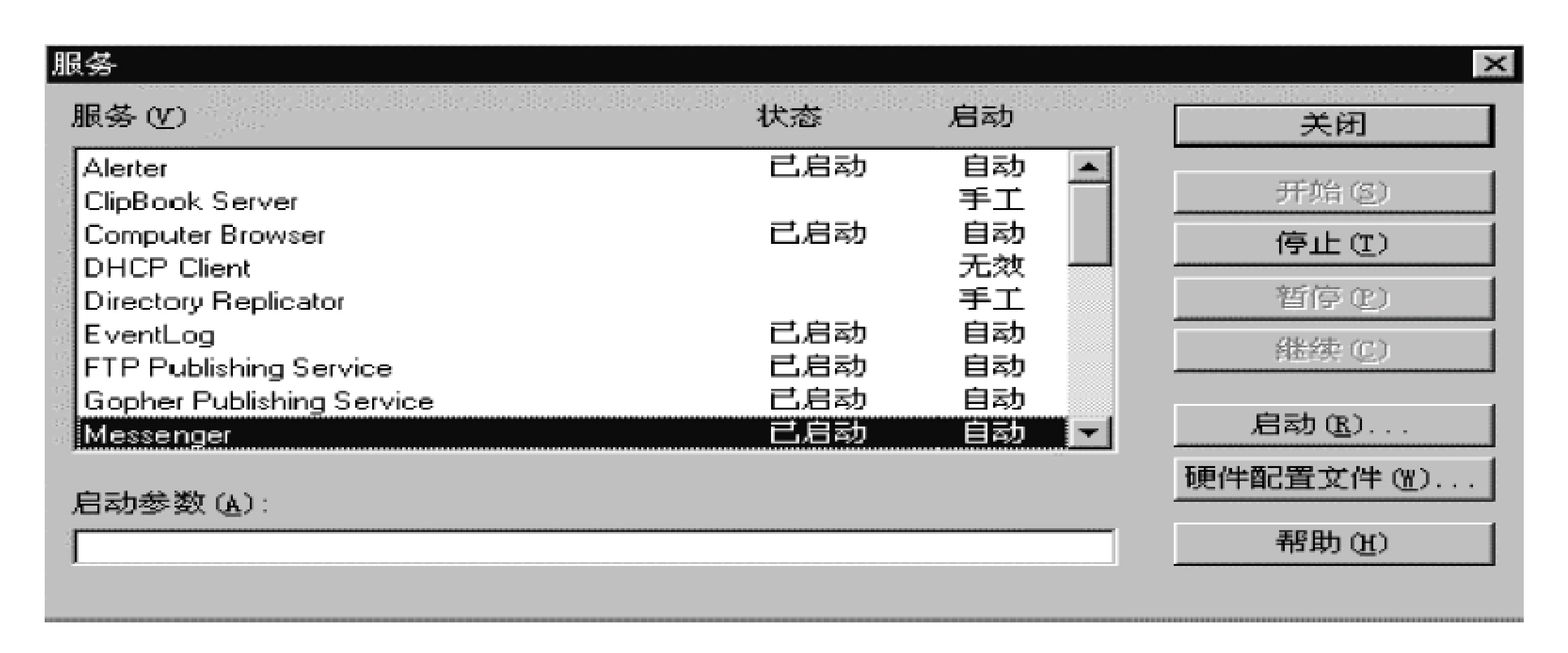


图 9-8 “服务”窗口

2. Windows 95/98 工作站中的信使功能

(1) 启动 Windows 95/98 的信使功能

在 Windows 95/98 中,启动信使功能就是指加载 winpopup.exe 程序,有两种启动 winpopup.exe 的方式。

实例 1 在启动 Windows 95/98 的同时加载指定程序 winpopup.exe。

① 依次选择“开始”→“设置(S)”→“任务栏和开始菜单程序”命令选项。

② 在打开的“任务栏 属性”窗口中,选择“开始菜单程序”选项卡,单击“添加”按钮,激活与图 9-9 类似的“快捷方式”向导窗口。



图 9-9 “创建快捷方式”向导窗口

③ 在“创建快捷方式”向导窗口中,单击“浏览”按钮,找到要启动的程序 winpopup.exe,单击“下一步”按钮。

④ 在“选择程序文件夹”窗口中,选择“启动”文件夹,单击“下一步”按钮,在激活的“选择程序标题”中,输入要加入到“启动”菜单中的程序名称后,单击“完成”按钮。如果 Windows 提示选择一个图标,请选择某个图标,如果没有提示请直接单击“确定”按钮,完成操作。

说明: 系统再次启动之后,可以自动启动图 9-10 所示的 WinPopup 窗口。

实例 2 在需要时,手动启动 winpopup.exe。

① 依次选择“开始”→“运行”命令选项，打开“运行”窗口。

② 在“运行”窗口中，单击“浏览”按钮。

③ 在激活的窗口中，找到或输入要启动的程序名 winpopup.exe 后，单击“确定”按钮，激活如图 9-10 所示的窗口。



图 9-10 WinPopup 窗口

(2) 启动设置 winpopup.exe 程序的步骤

① 按照上述方法启动 winpopup.exe 程序后，激活如图 9-10 所示的窗口。

② 在图 9-10 所示的窗口中，依次选择“消息(M)”→“选项(O)”命令选项，激活如图 9-11 所示的窗口，用户可根据需要酌情设置。

③ 设置之后，在图 9-11 所示的窗口中，单击“确定”按钮，操作完成。



图 9-11 选择“消息”→“选项”命令后的“选项”窗口

(3) 使用 winpopup.exe 发送弹出式消息的步骤

① 按照上述方法启动 winpopup.exe 程序后，激活如图 9-10 所示的窗口。

② 若要使用其发送弹出式消息，在图 9-10 所示的窗口中，依次选择“消息(M)”→“发送(S)”命令选项，激活如图 9-12 所示的窗口。

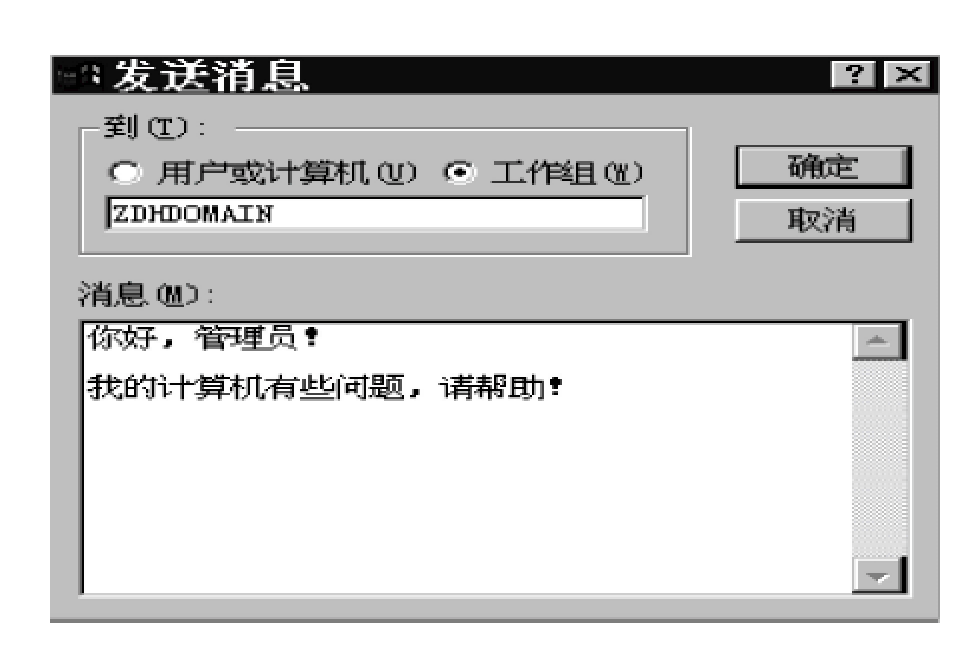


图 9-12 WinPopup 的“发送消息”窗口

③ 要向某个人发送一条消息，请在图 9-12 所示的窗口中，选择“用户或计算机”单

选钮。

④ 要向工作组中的每个人发送一条消息，请在图 9-12 所示的窗口中，选择“工作组”单选钮。

⑤ 在图 9-12 所示的窗口中，填写所要发送的消息正文，单击“确定”按钮，操作完成。发送成功后，将出现如图 9-13 所提示的信息。



图 9-13　WinPopup 中发送消息成功时的提示

3. 使用“MS-DOS 命令提示符”下的命令行信使功能

无论是在 Windows NT Workstation 还是在 NT Server 中，均可以使用命令行完成信使功能，其方法有两种。

(1) DOS 环境下发送消息命令行

① 依次选择“开始”→“程序”→“MS-DOS 命令提示符”命令选项，激活如图 9-14 所示的窗口。

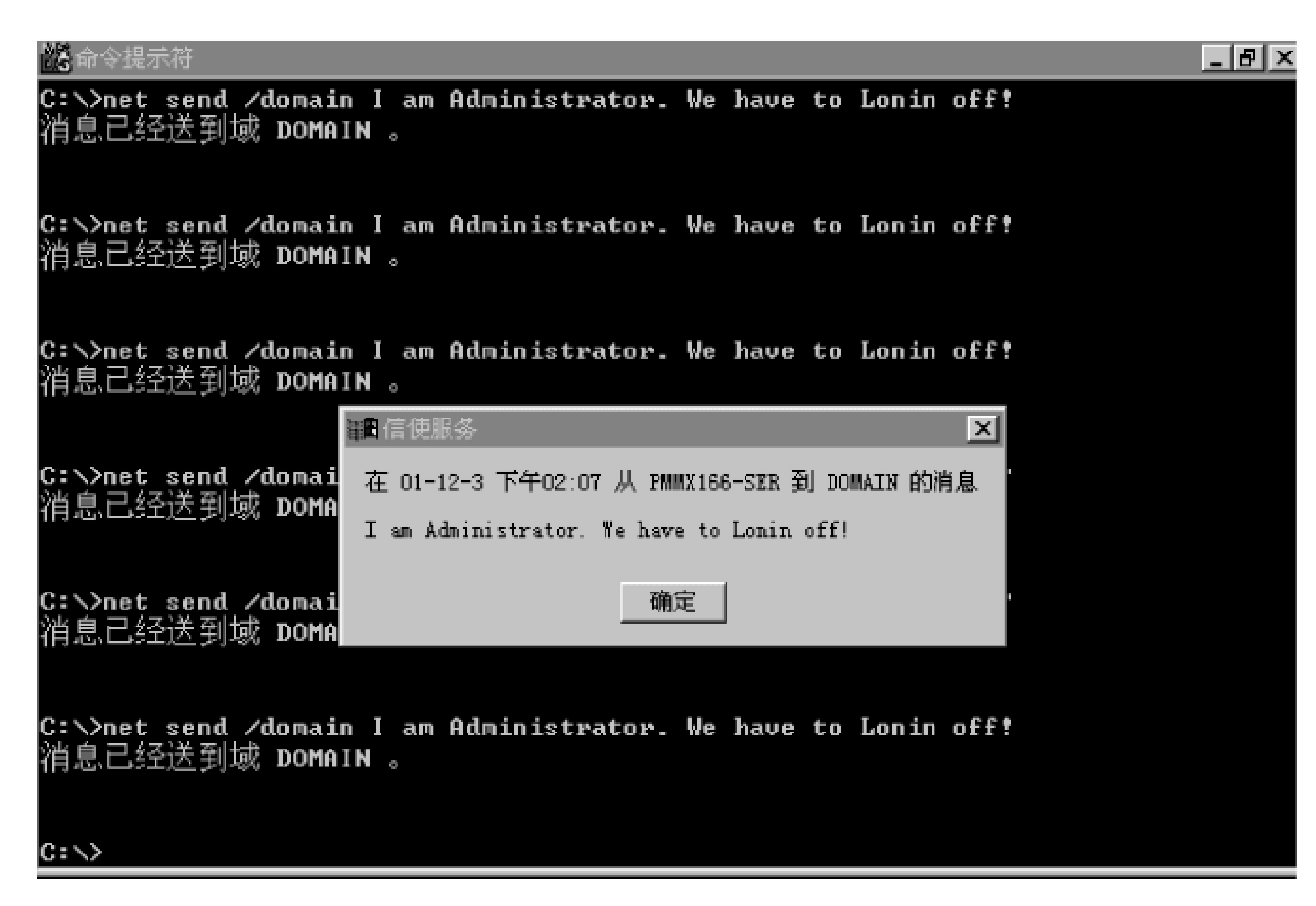


图 9-14　“MS-DOS 命令提示符”下发送的命令行和消息成功时的提示

② 在图 9-14 所示的窗口中，输入命令行“net send /domain 信息内容”后，按 Enter 键，即可将命令行中信息发送到指定的域中。

注意：此处参数“/domain”的含义是指发送信息到域中的所有计算机上，并不表示在此处输入所在域的域名。

(2) “运行”窗口运行命令行

① 依次选择“开始”→“运行”命令选项。

② 在激活的“运行”窗口中，输入命令行“net send /domain 信息内容”后，单击“确定”按钮，也可以将上述命令行中的信息发送出去。

③ Windows 98 和 NT Server 计算机上收到的信息如图 9-15 和图 9-16 所示。

注意：对于安装了 NT 系统的计算机，在发送警报和消息之前，必须在发送计算机上启动 Alerter 和 Messenger 服务。而对于接收警报与消息的计算机，则必须按上述不同环境的设置步骤设置之后，才能正确接收到警报与消息。

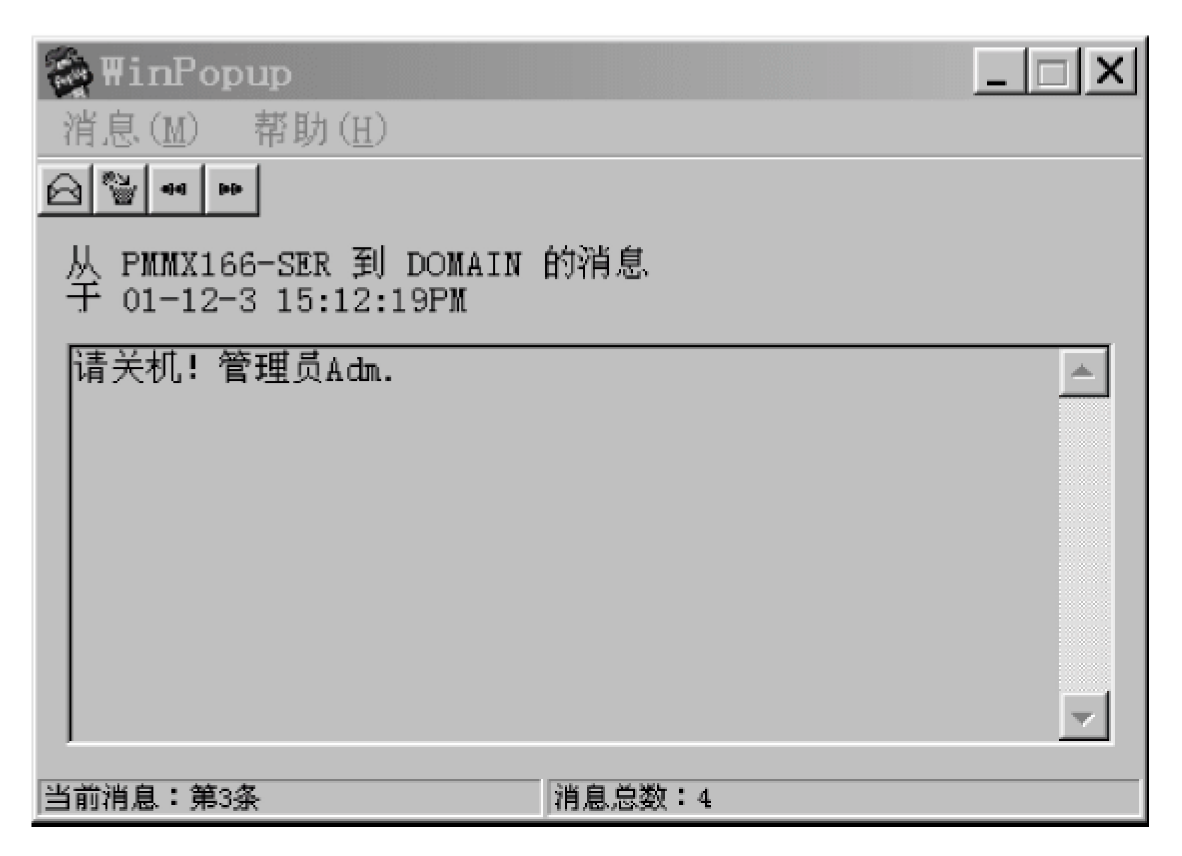


图 9-15 Win98 中接收到的信息



图 9-16 NT Server 中接收到的信息

9.5 管理域

本节介绍系统管理员在管理域时的基本操作。

9.5.1 备份域控制器(BDC)升级为主域控制器(PDC)

将“备份域控制器”(BDC)升级为“主域控制器”(PDC)的步骤如下：

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机列表中的备份域控制器。这应当是一台能可靠地处理高负荷网络传输负载的计算机。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“升级到主域控制器”命令选项。执行该命令之后，先前的“主域控制器”将自动降级为“备份域控制器”。

9.5.2 主域控制器(PDC)降级为备份域控制器(BDC)

将“主域控制器”(PDC)降级为“备份域控制器”(BDC)步骤如下：

① 在图 9-1 所示的“服务器管理器”窗口中，选定计算机列表中的“主域控制器”。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“降级为备份域控制器”命令选项。执行该命令之后，先前的“主域控制器”将降级为“备份域控制器”。

注意：通常，将“备份域服务器”升级为“主域控制器”之后，因为系统会自动将原“主域控制器”降级为“备份域控制器”，所以并不需要执行该操作。如果现有的“主域控制器”

不可用(如处于维修状态中)时,则可以将一个“备份域控制器”临时升级为“主域控制器”。当先前的“主域控制器”重新工作时,则必须将已升级的“主域控制器”重新降级为“备份域控制器”。

9.5.3 同步主域控制器和备份域控制器

打开“服务器管理器”,同步“主域控制器”和“备份域控制器”的步骤如下:

① 在图 9-1 所示的“服务器管理器”窗口中,选定计算机列表中的“主域控制器”。

② 在图 9-1 所示的窗口中,依次选择“计算机”→“与主域控制器同步”命令选项。

注意:同步通常由系统自动执行,但是如果运行 Windows NT Server 计算机中的目录数据库不同步,或者是“备份域控制器”由于密码失败而无法建立起网络连接时,则必须以手工方式完成同步操作。

9.5.4 将计算机添加到域

有时,需要将 NT Workstation 或普通的 NT Server 计算机加入到“域”,将计算机添加到域的步骤如下:

① 在图 9-1 所示的“服务器管理器”窗口中,选定计算机列表中的“主域控制器”。

② 在图 9-1 所示的窗口中,依次选择“计算机”→“添加到域(A)”命令选项后,激活如图 9-17 所示的窗口。



图 9-17 “添加计算机到域”窗口

③ 在图 9-17 所示的“添加计算机到域”窗口中,应根据所要加入计算机的类型,在“Windows NT 工作站或服务器”或者是“Windows NT 备份域控制器”两个单选钮中作出选择。

④ 在图 9-17 所示的窗口的“计算机名”文本框中,先输入计算机名,然后单击“添加”按钮。之后,便会将该计算机名所代表的计算机,添加到域的目录数据库中。

⑤ 之后,会激活一个新的类似于图 9-17 的窗口,与之不同的是,图 9-17 中间的“取消”按钮变为“关闭”。

⑥ 在图 9-17 所示的窗口中,单击“关闭”按钮,完成操作。

⑦ 该计算机将添加到“服务器管理器”的列表中。在添加计算机之后,系统只是将该计算机的用户添加到域。

注意：

- 对于一般的 NT 工作站和服务器，将计算机添加到域的操作，可以在该计算机上安装 NT 系统时完成，也可以在安装之后，按上述操作步骤执行后完成。而对于“主域控制器”，则只能在安装期间完成。
- 完成将计算机添加到域的操作时，必须使用本机管理员、域管理员、该域的账号操作员，或者是具有与上述各账号同等权限的账户身份登录。
- 完成将计算机添加到域的操作后，该计算机的图标呈现暗灰色。而在该计算机加入域之前，它的版本号和备注等信息在“服务器管理器”的列表中均不存在。
- 添加的计算机名将被视为网络的安全性因素。如果添加的计算机是服务器，当它加入域时会收到一份域目录数据库的副本。

9.5.5 从域中删除计算机

从域中删除计算机的步骤如下：

① 在图 9-1 所示的“服务器管理器”窗口中的计算机列表中，选定计算机，请勿选择无法删除的主域控制器。

② 在图 9-1 所示的窗口中，依次选择“计算机”→“从域中删除(R)”命令选项，或者直接按 Del 键。

③ 在激活的“服务器管理器”删除确认窗口中，单击“是(Y)”按钮，提示完成操作的信息。单击“确定”按钮，完成删除计算机的操作。

应指出的是，从域中删除的计算机上的用户，如果需要加入到其他的“域”或“组”中，则应在本机的“控制面板”的“网络”工具中删除原有域名或更改该域名，也可以更改为所要加入的域或工作组的名称。

9.6 控制面板内的服务器管理工具

NT 工作站和服务器的控制面板内提供了一些常用的管理工具，下面仅简单介绍其中的“启动/关闭”功能，读者如果对其他功能感兴趣，也可以自行操作，有困难的话可以随时查阅“帮助信息”。

启动服务器管理工具的步骤如下：

① 依次选择“开始”→“设置(S)”→“控制面板(C)”命令选项。

② 在打开的“控制面板”窗口中，选择“系统”图标，激活如图 9-18 所示的窗口。

③ 在图 9-18 所示的窗口中，可以改变多重引导时默认的启动系统，以及自动启动默认系统引导之前系统列表所等待的时间等项目的设置参数。例如，图 9-18 所示系统中的默认启动系统为 Microsoft Windows，启动时列表等待的时间为 15 秒(默认值为 30 秒)。当然，也可以直接修改 BOOT.INI 文件来实现此目的。

注意：使用“性能”选项卡，还可以实现对“虚拟内存”的设置，也可以对前台应用程序和后台应用程序使用 CPU 的时间长短等进行设置。

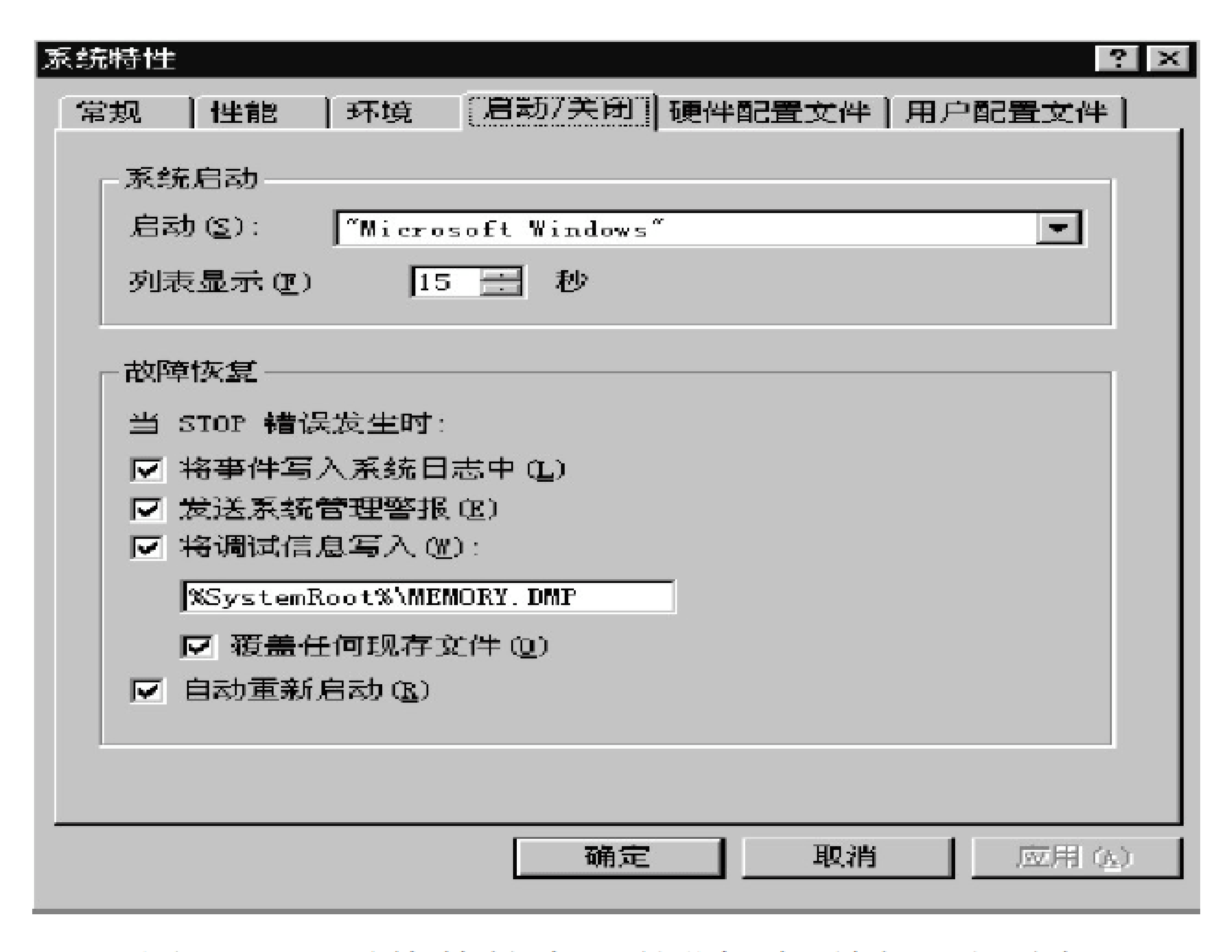


图 9-18　系统特性窗口的“启动/关闭”选项卡

习题

(1) 网络管理员在日常管理中,有哪些常规的管理工作?

(2) 在 NT Server 和 NT Workstation 中的基本管理工具各是什么? 分别具有哪些基本功能?

(3) 如何查看域内“主域控制器计算机”已连接的用户?

(4) 如何管理 NT 网络已连接的用户? “管理”的内容是什么?

(5) 什么是共享? 什么是会话? 如何管理它们?

(6) 什么是共享文件夹? 为什么要使用它?

(7) 在实施共享文件夹的过程中应当注意的要点有哪些?

(8) 管理共享目录的基本操作有哪些?

(9) 如何查看域内某计算机上连接和使用中的共享资源?

(10) 在 NT 网络中,如何对域内的共享资源进行管理? 管理的内容都有哪些?

(11) 当某个文件夹被共享之后,具有访问权限(许可)的用户可以访问什么?

(12) 对一个文件可以分配的访问权限(许可)有哪些? 每类许可所包括的允许的访问或操作有哪些?

(13) 共享文件夹的许可类型有哪些? 每类许可所包括的允许的访问或操作有哪些?

(14) 如何管理域内某计算机上的被使用的共享资源? 管理的内容都有哪些?

(15) 当用户访问某个共享资源失败时,应当如何检查? 解决的方法是什么?

(16) 在什么场合管理员需要给所管理的已连接计算机用户发送信息?

(17) 在 Windows 95/98 中给某计算机上的已连接用户发送信息的步骤有哪些?

(18) 如何将“主域控制器”降级为“备份域控制器”? 哪些用户有权进行上述操作?

(19) 什么时候需要将“备份域控制器”升级为“主域控制器”? 主要的步骤有哪些?

(20) 如何将普通的服务器改变为“主域控制器”？请叙述更改的主要步骤。

(21) 控制面板内的服务器管理工具有哪些？你会更改默认的启动系统吗？

(22) 什么是系统警报？如何指定接收警报的计算机和用户？

(23) 在 NT 和 Windows 95/98 中收到系统警报的条件是什么？

实训题目

1. 使用“服务器管理器”查看和管理组内计算机“连接中”的用户、用户会话、共享资源和“使用中”的资源情况。例如：管理(断开)某位用户会话的连接。

2. 在各种计算机平台(Windows 98/Me/NT/2000)上设置和使用信使功能,互相发送信息和给域或组中的计算机发送信息。

3. 使用“服务器管理器”将 NT Workstation 和 Windows 98 计算机加入到域。

4. 利用系统工具中的“启动/关闭”选项卡,使多重系统启动时的默认顺序分别为“Windows 98、NT Workstation、NT Server”,启动列表的等待时间改变为 10 秒。

5. 设置、使用和管理共享资源(文件和目录)。

① 开放一个共享名为“A1＄”和“A2”的共享资源,比较它们的使用区别。

② 为管理员和普通用户分别开放同一个文件目录,使得管理员具有“完全控制”的权限,而普通用户只有“读取”的权限。



Intranet 信息网站的建设与管理

本章将介绍创建 Intranet 信息网站必不可少的知识，包括：WWW、DNS、FTP 服务器和虚拟主机等概念。此外，还要详细地介绍 Internet/Intranet 信息网站管理员应当熟练掌握的创建、使用和管理 Web、FTP、DNS 服务器所必备的基本技能。

主要内容：

- Intranet 信息网站基础和基本概念；
- 虚拟主机的概念与配置；
- IIS4.0 中 DNS 服务器的建立、配置和使用；
- IIS4.0 中信息服务器的建立、配置和管理；
- IIS4.0 中的 Internet 服务管理器的启动和使用；
- 各种客户机对 WWW 服务器的访问；
- 各种客户机对 FTP 服务器的访问。

10.1 Intranet 信息网站概述

随着 Internet /Intranet 的广泛使用，C/S 网络模式已经发展为最新的 B/S 模式，WWW 服务也自然成为 Internet 和 Intranet 的核心。为此，与 WWW 信息浏览服务相关的技术需求与日俱增。许多单位和个人都需要建立和使用自己的网站，并通过 WWW 服务器向 Internet、Intranet 和 Extranet 上的众多用户提供 WWW 信息服务。因此，IIS 信息网络及其相关服务器的创建、管理和使用已经成为每个网络管理员必须掌握的基本技能。

1. B/S 浏览器/服务器网络结构(browser/server)

B/S 的全名为浏览器/服务器网络结构，它有许多显著的优点，例如，成本低、易于更新、用户可以自行安装浏览器软件、使用通用的浏览器进行信息访问、客户端软件廉价、安全保密性强以及控制灵活等。

2. Internet Explorer 浏览器

Microsoft Internet Explorer，简称 IE。它是一种 Web 浏览器。Internet Explorer 是

导航、访问和浏览 Web 网站信息的工具。它是 B/S 网络模式中客户机上安装的主要软件。当然，除了微软的 IE 外，还有网景公司的 Netscape Communicator 等许多类似的浏览工具，用户可根据习惯选用自己喜爱的工具。Internet Explorer 中的工具栏为管理浏览器提供了许多详细的功能和命令。工具栏下面的地址栏显示当前 Web 页的地址。要想到达新的 Web 页，可以直接将该页的 URL 地址键入此栏的空白部分，然后按 Enter 键，也可通过单击页面的“超级链接”跳转到新的页面。

10.2 微软的 Internet 信息服务器

为了适应目前 Internet/ Intranet 的潮流，各公司纷纷推出自己的产品，IIS 就是微软推出的相应产品。IIS 是 Internet information server 的英文缩写，其中文名称为“Internet 信息服务器”。在微软推出的众多应用产品和开发工具中，有许多是免费提供给用户使用的，微软也因而占有了很大的市场份额。在 Windows NT Server 4.0 中内置的产品名称为 IIS 2.0。目前，常用的产品是 IIS 4.0/5.0 版本。

10.2.1 虚拟主机的概念

1. 虚拟主机(virtual host)技术

IIS 采用的虚拟主机技术是目前 Internet/Intranet 上最常使用的一种技术与方法，其特点是通过 IIS 来配置多个虚拟主机，以实现一个 IP 地址对应多个虚拟主机的目标。使用虚拟主机技术的主要目的是解决 IP 地址紧缺的问题。

目前，常用的虚拟主机技术是通过一个 IP 地址来对应多个主机域名或主机名的，例如：使用这种虚拟主机技术，可以在一台计算机上，使用一个 IP 地址来对应需要安装的多台 WWW 服务器、FTP 服务器和邮件服务器等。这些具有不同主机名，而使用同一 IP 地址的计算机主机就被称为“虚拟主机”。

2. 虚拟主机的形式

虚拟主机通常有以下两种形式。

① 基于 IP 地址　这种形式要求每一个虚拟主机都具有一个 IP 地址，实现起来较为困难。早期的 WWW 服务器使用的就是基于这种技术的虚拟主机技术。

② 基于主机名　该方法提供了一种在一台主机上运行多个(无数)虚拟主机的技术。由于 IP 地址的紧缺，目前多数系统使用了基于主机名的虚拟主机技术。

3. 虚拟主机的配置

虽然不同系统配置虚拟主机的方法有所不同，但是都不复杂。在 IIS 中设置虚拟主机的步骤也很简单，在下一节中会作详细介绍。

10.2.2 Internet 信息服务系统的概述

IIS 是 Microsoft 为开发和建立 Internet 服务器所提供的基本软件组件。IIS 2.0 随 Windows NT Server 4.0 一起提供给用户，它只是一个简单的个人入门级的产品。而 IIS

3.0 只是在 IIS 2.0 的基础上增加了 ASP(active server pages)的设计和测试平台。只有使用 IIS 4.0,NT 网络的系统管理员才可以建立起大容量、功能强大的 WWW、FTP 和 Gopher 服务器,从而拥有属于自己的、安全的 Internet 和 Intranet 网站,并将信息发布给全世界的用户。

IIS 4.0 是 NT Server 4.0 的附加软件包 Option Pack 的一部分。IIS 4.0 与 NT Server 紧密集成在一起,提供了建立 Intranet 网站所必需的几乎所有功能,并且还提供了一套系统管理工具,以及建立 web 应用程序的基本构件。

1. IIS 的特点

① 高性能的网络应用程序开发平台。

② 集成了全文本搜索能力。

③ 支持多媒体技术。

④ 具有站点的管理能力。

⑤ 可以将结构化查询语言(SQL)数据转换为超文本标记语言(HTML)格式。

2. IIS 可实现的功能

① 发布商业信息、销售信息、企业信息广告等主页。

② 提供交互式页面文件,可以设计调查问卷、接受定单等。

③ 提供远程销售,使得用户可以更容易地访问销售数据库。

④ 使用定单跟踪数据库。

⑤ 通过 Internet 数据库连接器(Internet database connector,IDC),可以使 WWW 服务器与数据库相结合实现多查询和多连接。

⑥ 通过 Microsoft Internet Server 应用程序编程接口(ISAPI),可以创建高性能的客户/服务器应用程序。

⑦ 发布交互式程序。

⑧ 可以通过创建 ISAPI 筛选程序来自定义 WWW 服务。此筛选程序还可以侦听到输入或输出的请求,并自动执行动作。例如增强的记录。

⑨ 可以运行公用网关接口(CGI)应用程序。

⑩ 可以使用 FTP 服务器发送或接收文件。

3. IIS 包括的组件

① Internet 服务　可提供 WWW、FTP 和 Gopher 等多种服务。

② Internet 服务管理器　为管理 Internet 服务提供了工具。

③ Internet 数据库连接器　向数据库发送查询的组件。

④ 密钥管理器　用于安装安全套接字层(SSL)密钥的工具。

上面提到的 Gopher 服务器,即信息查寻和检索服务器,建立之后,用户就可以使用 Gopher 协议从 Internet 和 Intranet 上的此类服务器上查寻和搜索文件,目前已很少应用了。

4. IIS 的工作过程

如图 10-1 所示,WWW 服务子系统是基于客户/服务器模式的服务请求和响应系统。WWW 浏览器接收 URL 中发送给 WWW 服务器的服务请求信息。WWW 服务器接受

请求后，进行处理，并通过浏览器将超文本标记语言（HTML）方式的页面的结果信息，返回给客户机上的用户。

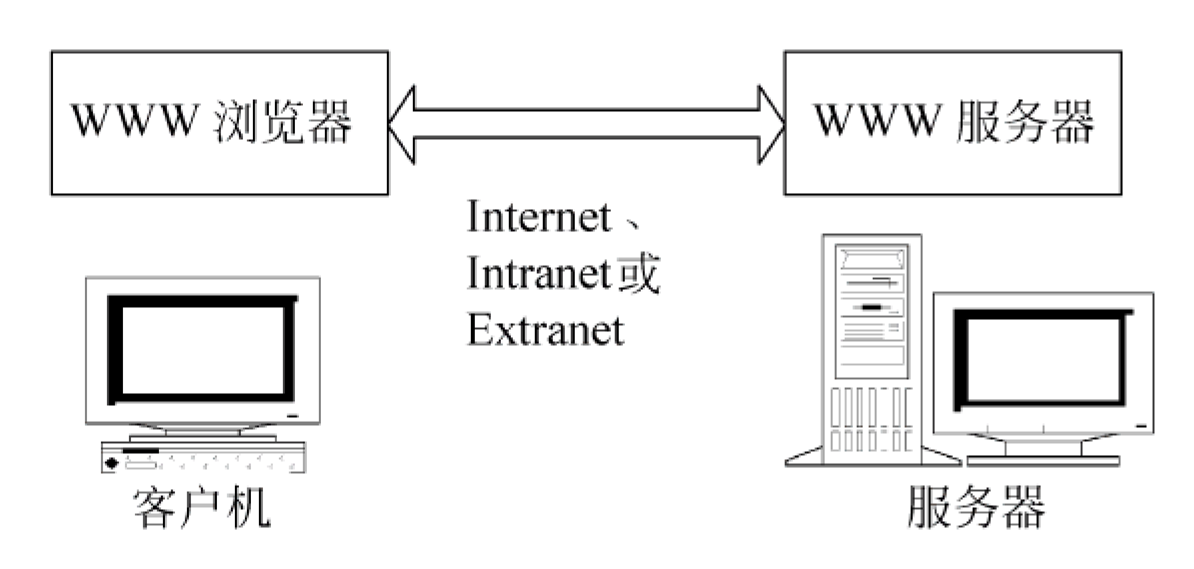


图 10-1　IIS 的工作过程

5. Intranet 的组建

第 5 章中已经介绍了 Intranet 的规划、设计以及建设过程，下面开始讨论如何利用 NT 来建设和实现一个 Intranet。在一个实用的 Intranet 信息网络中，除了应当具有 DHCP 服务系统、邮件服务系统和打印服务系统之外，最重要的就是 WWW 服务系统、FTP 服务系统、DNS 服务系统和 RAS 远程访问服务系统等。

在较小的 Intranet 中，可以将 Internet Information Server 添加到现存的工作组服务器或者打印服务器上形成非专用的 WWW 服务器。该服务器允许将个人 Web 样式的页面、自定义的应用程序作为宿主，并结合结构化查询语言（SQL）数据库的界面，实现信息资源的访问。用户还可以使用远程访问服务（RAS）从远程节点上对信息资源进行拨号访问。

在具有多个部门或工作组的大企业中，可以在每个部门现有的 PDC 服务器上，运行 Internet Information Server 形成专用的中央信息服务器，该 IIS 服务器可提供公司内外范围的信息查询、访问和管理，例如，提供员工手册、产品信息、共享数据或公司目录等信息资源。

6. 使用 IIS 建立 Intranet 网站的过程

（1）需要管理的模块

网络管理员在进行系统配置管理时，对于每种服务子系统均可以按以下 3 个模块分别进行。

① 服务器端的安装与配置管理。

② 客户计算机端的安装与配置管理。

③ 服务器端对相应服务的管理。

（2）配置的过程

对于选定的 WWW、DNS 和 FTP 服务子系统来说，配置应当按下述过程分别进行：

① 服务器端的配置。

- 在 NT Server 的“控制面板”窗口打开“网络”窗口，分别安装两种网络服务，即安装 DNS 与 NT Server 内置的 IIS 2.0（含 WWW 和 FTP），或者单独安装 IIS 4.0。
- 配置 DNS 域名服务器。
- 配置 WWW 服务器。

- 发布主页到 WWW 服务器预定的位置。
- 配置 FTP 服务器。
- 将网络内部的共享文件和目录放置到 FTP 服务器指定的位置。
- 如果需要,安装代理服务器。

② 客户机端的设置。对于选定的 WWW、DNS 和 FTP 服务子系统来说,客户机端都应当进行相应的配置。

③ 服务管理。各种服务子系统的管理也可以按照上述层次分别进行。

10.3 建立、配置和使用 IIS 4.0 版本的信息服务器

如前所述,真正能够满足企事业单位需要的应当是 IIS 4.0 或 IIS 5.0。它们在与 NT Server 紧密结合的基础上,提供了组建一个 Intranet 网络所必需的几乎一切功能,而且还提供了一套系统管理工具和建立 Web 程序的基本构件。

10.3.1 获得 IIS 4.0 的途径

获得 IIS 4.0 的途径有以下两个:

方法 1:对于使用正版软件的用户,使用自带的"Option Pack 4.0"光盘。

方法 2:如果用户已经有了 NT Server,但是没有 IIS 4.0,则可以使用浏览器,访问下述网址免费下载。

- http://www.Microsoft.com/downtrial/optionpack.asp
- http://www.Microsoft.com/iis

10.3.2 安装 IIS 4.0

1. 安装 IIS 4.0 的条件

(1) 硬件准备

硬件准备条件与安装 NT Server 软件的平台条件类似即可。

(2) 软件准备

在安装 IIS 4.0 之前,应做好如下准备工作:

① Windows NT 4.0 Server 光盘,或者从该光盘复制所有的 I386 目录文件到硬盘上。

② Windows NT 4.0 Option Pack 光盘。

③ IE4.0 以上版本的浏览器软件。

④ Windows NT Server 4.0 的补丁程序 SP3~SP6,一般在 NJ-WS 光盘内。

(3) 安装前的准备

① 在安装 IIS 4.0 之前,应先关闭安装在 NT Server 4.0 上的其他版本的 WWW、FTP 和 Gopher 服务,以及 Windows NT Resource Kit 中的 Windows Academic Centre (EMWAC)服务。之后,删除旧版本的 IIS,例如 IIS 2.0/3.0。

② 需要安装如下软件：

- 安装 Windows NT Server 4.0。注意，对于那些需要文件安全级的网络用户，应当使用 NTFS 格式进行安装。
- 安装 Windows NT Server 4.0 的 SP3～SP6 中的一个软件，推荐安装的版本为 Server Pack 4 或 Server Pack 5。如果安装启动后，出现蓝屏的现象，请立即按“空格”键恢复上一次的正确配置，即可放弃刚刚安装的补丁程序，正常进入原来的系统。然后，降低补丁程序的版本重新安装，直至成功。
- 安装 IE 4.0 以上版本的浏览器软件。

③ TCP/IP 是用来建立 Internet 连接，并从 Internet/Intranet 上查询和获取数据时使用的主要协议，因此，应当在 Windows NT 网络的服务器和客户机上分别安装、配置 TCP/IP 协议。

2. 安装 IIS 4.0 的方式

安装 IIS 4.0 有以下几种方式：

① 替换安装　就是用新的版本替换原有的 IIS 版本，并且补充安装一些必要的附加程序。采用这种方式时，会同时安装索引服务器（index server），使用该项服务，用户可以查询本地网点上的数据。

② 升级安装　就是在旧版本的基础上进行添加式的升级安装。用户使用这种方式安装时，并不删除原有的部件，只需从选单列表中，选择需要安装的部件。

③ 全新安装　需要完全删除旧版本的 IIS，再重新安装 IIS 4.0。本书介绍的就是这种安装方式。

3. IIS 4.0 的安装步骤

① 在 NT Server 的 CD-ROM 中放入正版软件自带的“Option Pack 4.0”光盘后，会自动启动安装程序。

② 进入启动菜单后，选择其中的“5”，即选中安装 Windows NT 4.0 Option Pack 的选项；也可以双击其中的 Setup 程序来启动安装向导，激活如图 10-2 所示的窗口。

③ 在图 10-2 所示的窗口中，单击“是(Y)”按钮，激活如图 10-3 所示的窗口。



图 10-2　Windows NT 4.0 Option Pack“安装程序”窗口

④ 在图 10-3 所示的窗口中，单击“确定”按钮，激活后继的窗口。

⑤ 在激活的下一个窗口中，单击“下一步(N)”按钮。当出现最终用户许可协议的询问窗口时，单击“接受按钮”，接受协议所述内容；然后，单击“下一步(N)”按钮。

⑥ 当出现“选择安装的方式”窗口时，用户可根据需要进行选择。例如单击“典型”按钮，选择典型安装方式；最后，单击“下一步(N)”按钮，激活如图 10-4 所示的窗口。



图 10-3　Windows NT 4.0 Option Pack IIS 4.0 安装向导



图 10-4　Microsoft IIS 4.0 安装程序

⑦ 当出现图 10-4 所示的窗口时，可以根据需要选择主目录，若直接单击"下一步(N)"按钮，即选择了系统默认的主目录。

⑧ 当出现安装完成的提示窗口时，单击"完成"按钮，完成 IIS 4.0 的安装。

⑨ 重新启动计算机后，安装生效。至此，IIS 4.0 的安装过程结束。

10.3.3　DNS 服务器的建立与设置

1. DNS **概述**

在 Internet 环境中，人们为了通信必须知道各自的计算机地址，但是对于那些枯燥且无意义的 IP 地址是很难记住的，而为了使用 Internet 上的各种资源，又必须使用计算机能够识别的 IP 地址或计算机的物理地址，因此，在 Internet 中使用了一整套规则来表示 Internet 上的计算机的地址，这就是"域名系统"(DNS，domain name system)。有了 DNS 服务和 TCP/IP 协议，当用户在 Internet 上浏览和使用资源时，就无需记忆"IP 地址"或"物理地址"，而只需知道它的名称。例如，浏览"NBA"中文网页时，只要键入"www.nba.com.cn"，即可进入它的主页。这就像使用不同语言国家的人们交流时必须经过翻译一样，在网络中负责翻译工作的计算机就是 DNS 服务器，它具有如下功能：

① 具有"主机"(网络上的计算机)及其对应"IP"地址的数据库。

② 可以接受 DNS 客户机提出的"主机名称"对应 IP 地址的查询请求。

③ 查询所请求的数据，若不在本服务器中，能够自动向其他的 DNS 服务器查询。

④ 向 DNS 客户机提供其“主机名称”对应的 IP 地址的查询结果。

2. 在 NT Server 中安装 DNS 服务器

为了实现 DNS 服务器的功能，系统中应该安装有 DNS 服务器。

检查 NT Server 4.0 中是否安装了 DNS 服务的步骤如下：

① 在 Windows NT 任务栏上，依次选择“开始”→“设置”→“控制面板”命令选项。

② 在打开的“控制面板”窗口中，双击“网络”图标，选择其中的“服务”选项卡。在该窗口中，就可以检查是否已经装载了“Microsoft DNS 服务器”选项，如果没有，单击“添加”按钮。安装之后，在管理工具中应当增加了“DNS 管理器”，系统管理员可以利用它来管理 DNS 数据库和 DNS 的服务。至此，检查是否已安装 DNS 服务的过程结束。

3. 在 IIS 4.0 中使用 DNS 管理器配置 DNS 服务器的总体步骤

① 选择或添加一个 DNS 服务器。

② 新建一个区域(zone)。在输入区域名称之后，NT Server 会为此生成对应的区域文件。

③ 在所建区域中建立记录。所建的记录应当包含以下几种类型：

- NS 记录　用来记录此域中的 DNS 服务器，即指明该区域使用的 DNS 服务器。例如，输入 NTServer.zdh.com.cn。
- SOA 记录　用来指明该区域网管员使用的电子邮件信箱。
- A 记录　用来记录主机的 IP 地址。例如，输入 DNS 服务器主机的 IP 地址为“202.112.144.20”。
- CNAME 记录　用来为主机创建别名，使客户机的客户可以通过主机的“别名”来访问主机。例如，输入“WWW”为别名。
- MX 记录　用来定义处理网上电子邮件的 DNS 服务器。

4. 在 IIS 4.0 的 DNS 管理器中建立与设置 DNS 服务器的具体配置

(1) 创建 DNS 服务器

① 依次选择“开始”→“程序”→“管理工具(公用)”→“DNS 管理器”命令选项，打开如图 10-5 所示的窗口。在该窗口中，选择“DNS”→“新建服务器”命令选项，激活对话框。

② 在图 10-5 中所示的“添加 DNS 服务器”对话框中，输入 DNS 服务器对应的 IP 地址，然后单击“确定”按钮。

完成添加 DNS 服务器后的“域名服务管理器”窗口如图 10-6 所示。

(2) 新建一个区域(zone)

① 依次选择“开始”→“程序”→“管理工具(公用)”→“DNS 管理器”命令选项，激活如图 10-6 所示的窗口。

② 在图 10-6 所示的窗口中，依次选择 DNS→“新建区域”命令选项，激活如图 10-7 所示的窗口。

③ 在图 10-7 所示的“为 202.112.144.20 创建新区域”窗口中，选择“区域类型”单选钮的“主要”，单击“下一步”按钮，激活如图 10-8 所示的窗口。

④ 在图 10-8 所示的窗口中，输入要求的信息后，单击“下一步”按钮。

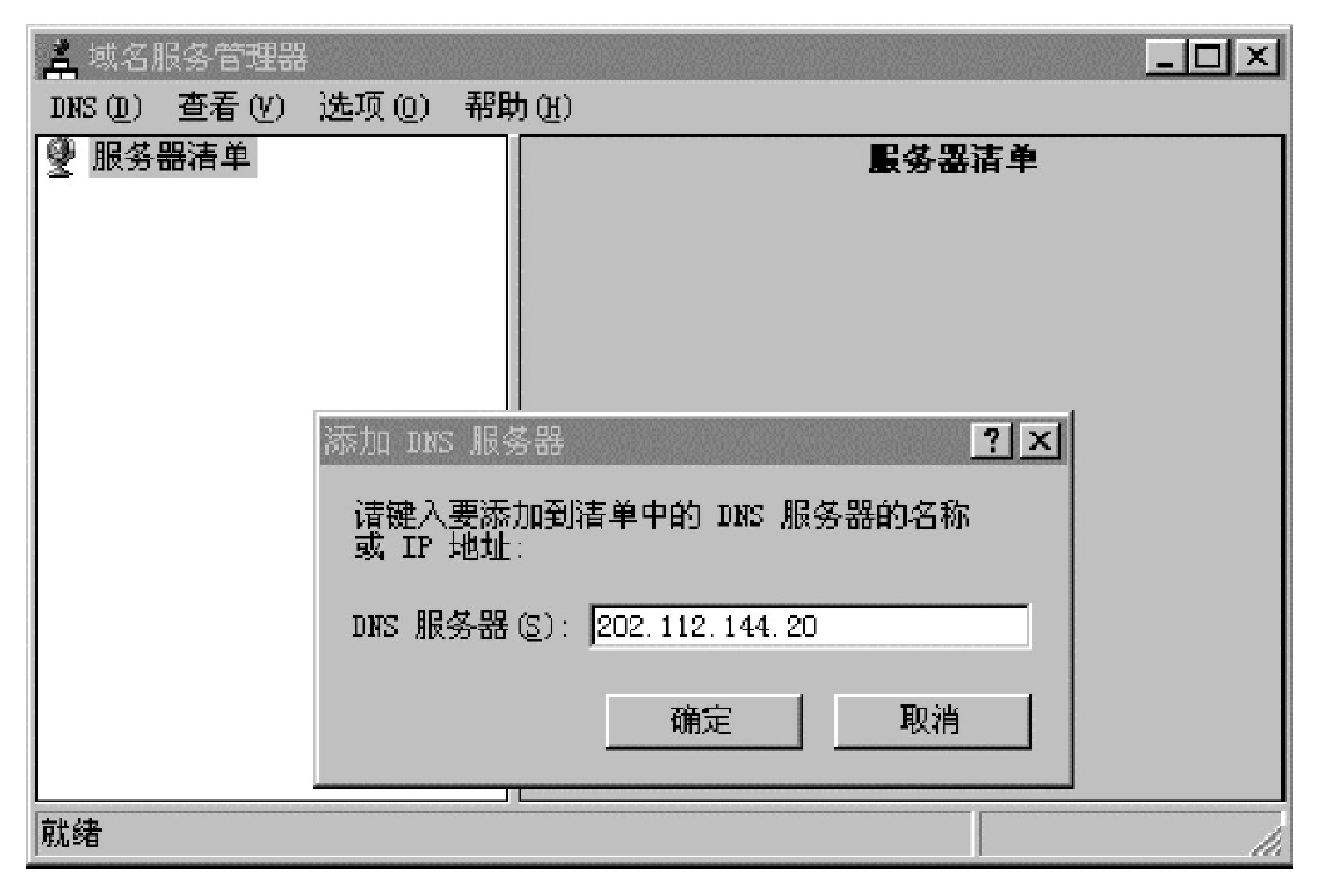


图 10-5　“域名服务管理器”和“添加 DNS 服务器”窗口

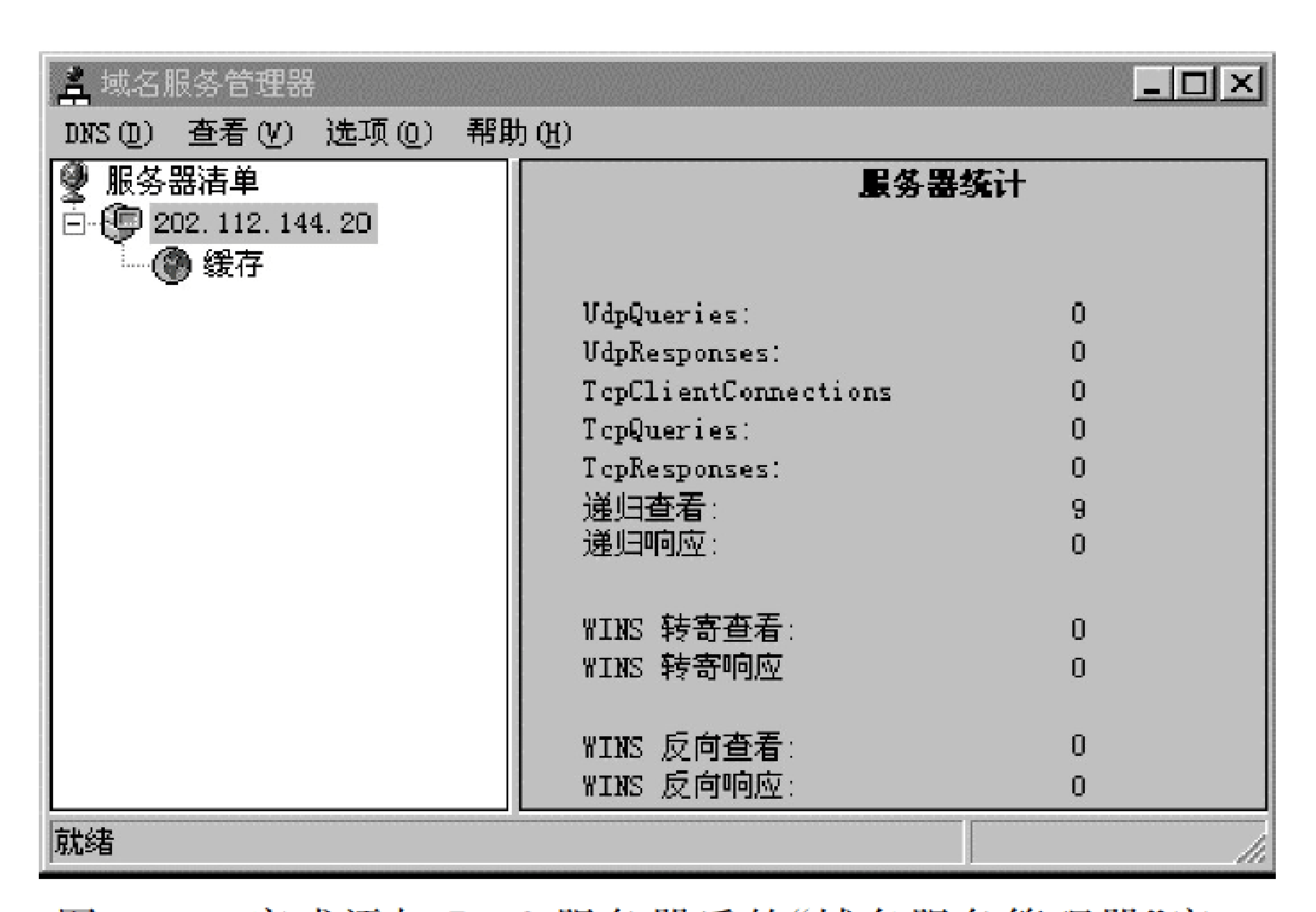


图 10-6　完成添加 DNS 服务器后的“域名服务管理器”窗口

为 202.112.144.20 创建新区域

区域类型

主要 (P)

辅助 (S):

区域 (E):

服务器 (R):

< 上一步 (B)　下一步 (N) >　取消

图 10-7　“为 202.112.144.20 创建新区域”窗口

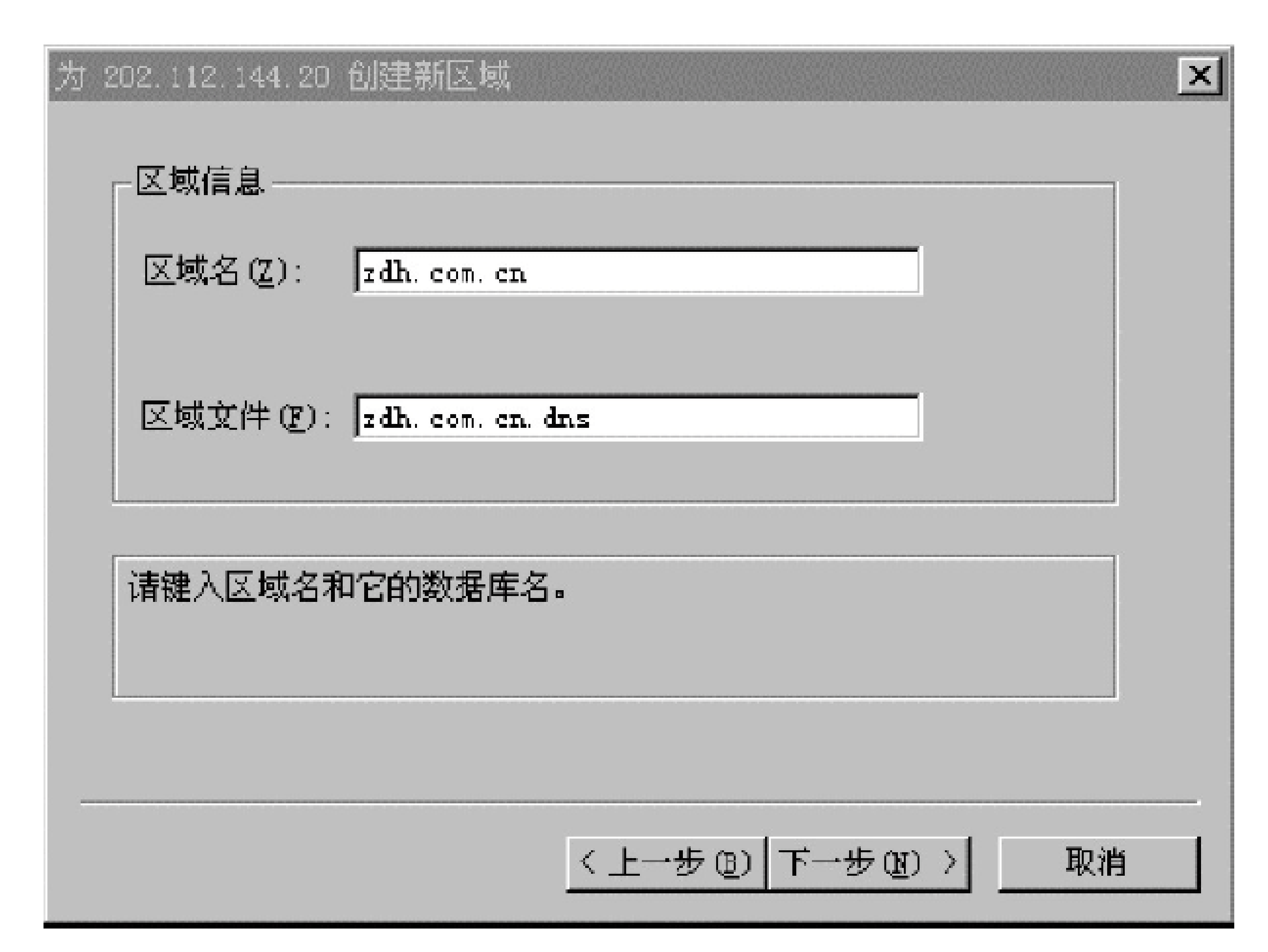


图 10-8 “创建新区域”窗口

⑤ 当提示输入已经完成时，单击“完成”按钮，完成“创建新区域”。

(3) 创建记录

在创建区域之后，还要在所建的区域中建立记录。此时的“域名服务管理器”如图 10-9 所示，应该已经存在 NS、SOA 和 A 记录，如果没有则应逐一添加。添加记录的方法如下：

① 在图 10-9 所示的“域名服务管理器”窗口中，选择 DNS→新建记录”命令选项，激活如图 10-10 所示的窗口。



图 10-9 完成“创建区域”之后的“域名服务管理器”窗口

② 在图 10-10 所示的“新建资源记录”窗口中，在“记录类型”列表框中选择“CNAME 记录”选项，在窗口右边输入有关 WWW 服务器的信息后，单击“确定”按钮，返回图 10-9 所示的窗口，此时，窗口已经新增加了 CNAME 记录。

说明：“新建资源记录”窗口中的“DNS 名称”可以使用 IP 地址，也可以使用已建立的域名。

③ 在图 10-9 所示的“域名服务管理器”窗口中，再次选择“新建记录”选项，激活如图 10-11 所示的窗口。

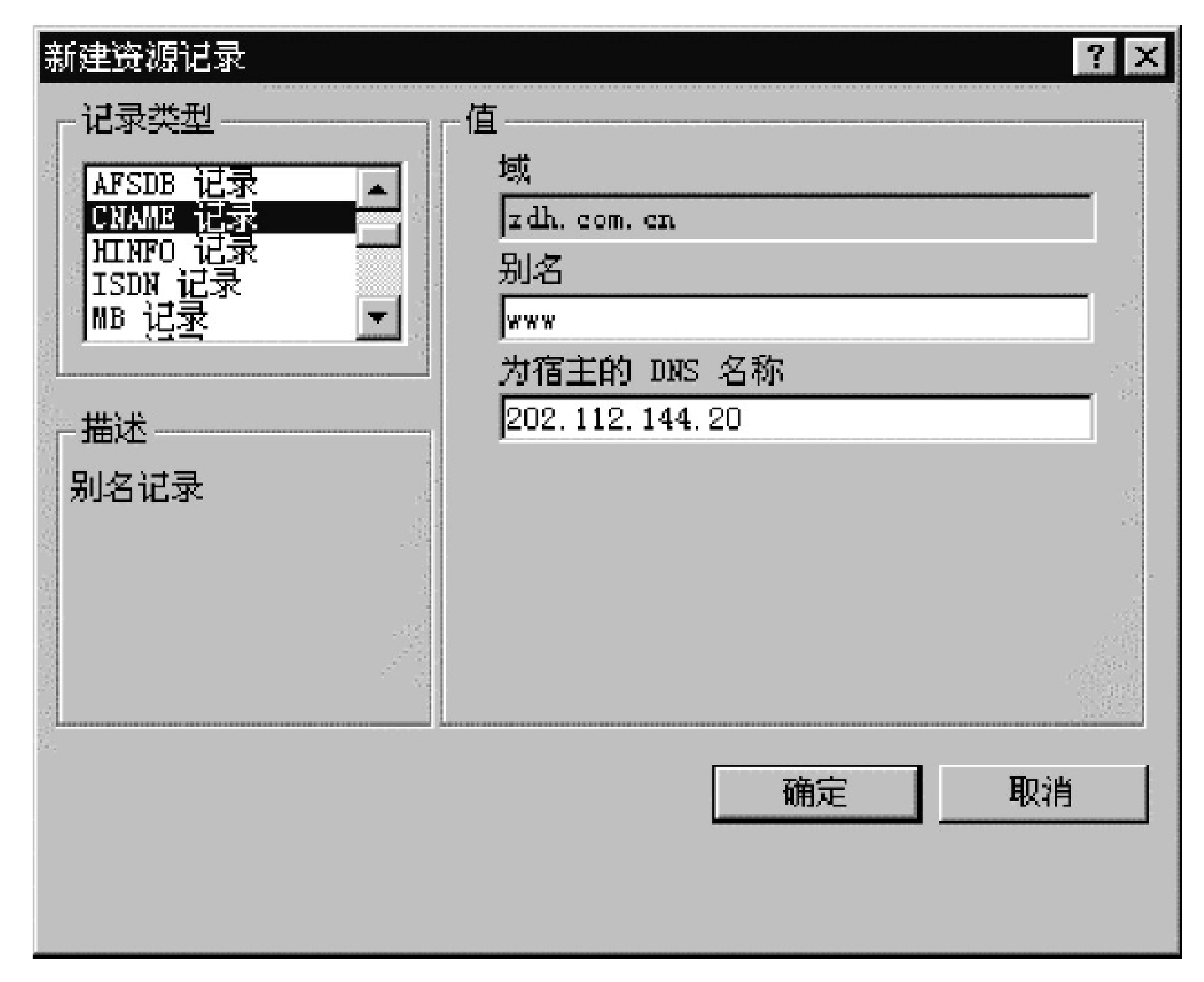


图 10-10 “新建资源记录”——使用 IP 地址建立 WWW 记录的窗口



图 10-11 “新建资源记录”——使用 IP 地址建立 FTP 记录的窗口

④ 在图 10-11 所示的窗口中，在“记录类型”列表框中选择“CNAME 记录”选项，在窗口右边输入有关 FTP 服务器的信息后，单击“确定”按钮，返回图 10-9 所示的窗口。

⑤ 完成“创建区域”和新建资源记录之后的“域名服务管理器”窗口应显示所有记录的有关信息。

5. 设置 DNS 服务器本机的 TCP/IP 协议以验证 DNS 的工作

安装之后，应该对 DNS 服务器本机的 TCP/IP 协议进行设置，以验证 DNS 的工作情况。

① 在“控制面板”中打开“网络”窗口，选择“协议”选项卡，激活如图 10-12 所示的窗口。

② 在图 10-12 所示的“协议”选项卡中，选择“TCP/IP 通信协议”，单击“属性”按钮，激活如图 10-13 所示的窗口。

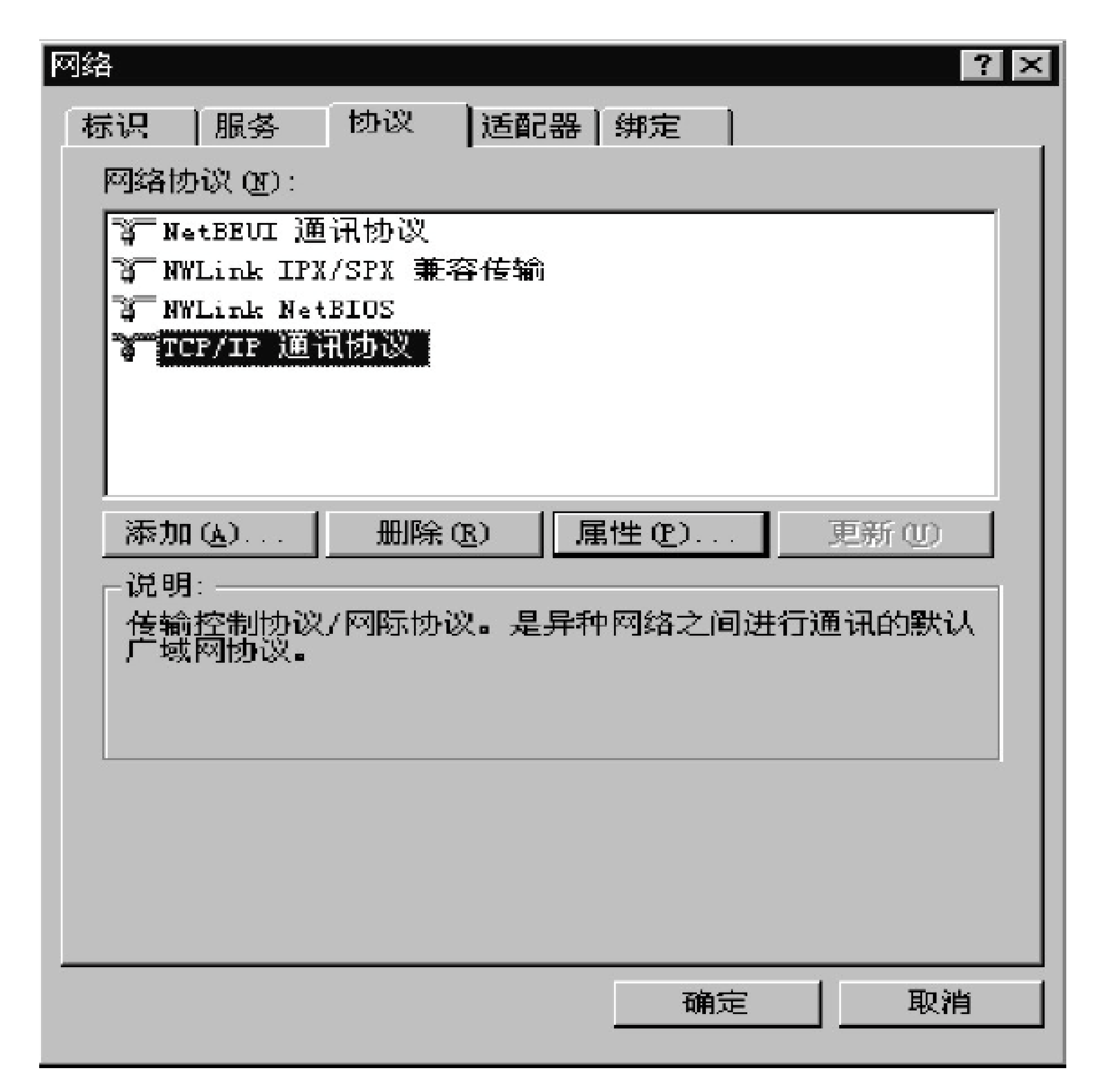


图 10-12 “网络”中的“协议”选项卡

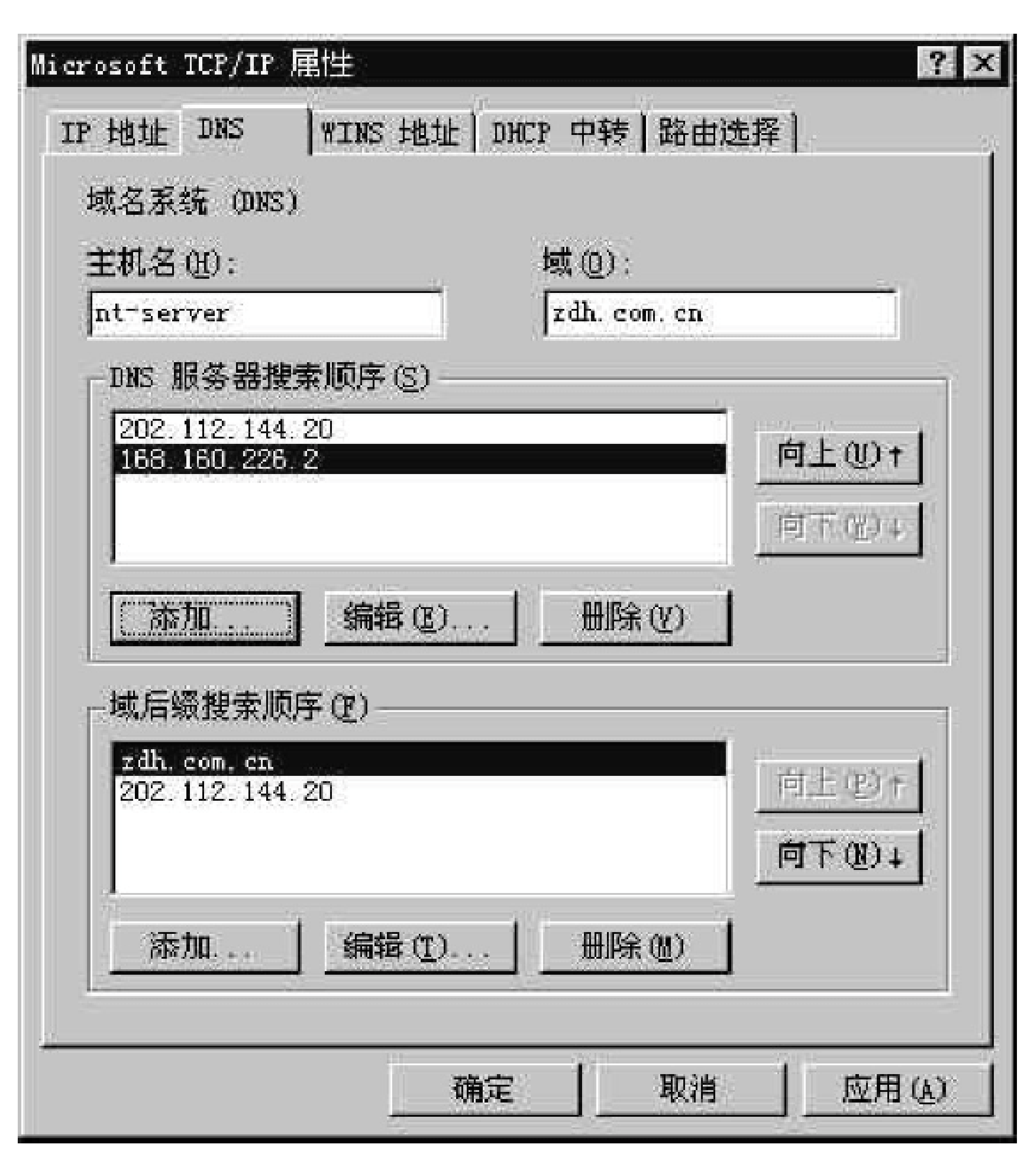


图 10-13 Microsoft TCP/IP 属性——DNS 选项卡

③ 在图 10-13 所示的“Microsoft TCP/IP 属性”窗口中，选择 DNS 选项卡，可以在“主机名”下的文本框中输入该 DNS 服务器的主机名称；在“域”的文本框中输入域的后缀；在“DNS 服务器搜索顺序”栏中添加 DNS 服务器的 IP 地址。完成之后，单击“确定”按钮，重新启动计算机。

至此，有关 DNS 服务器的基本设置完成。如果需要对上述参数进行修改，可以打开相应的窗口。在 NT 网络中，各种客户机在访问 WWW 服务器的主页之前，都必须对其安装的 TCP/IP 协议的 DNS 部分做必要的设置，否则不能使用域名对服务器中的资源进

行访问。

10.4 IIS 4.0 的配置和管理

Internet 服务管理器是一个管理工具。它的主要作用是监视、配置和控制 Internet 服务。

Internet 服务管理器处于信息管理的中心,通过它可以控制和组织所有运行 Internet Information Server 的计算机。Internet 服务管理器不但可以在 Windows NT Server 和 NT Workstation 上运行,还可以从其他计算机通过网络连接到 WWW 服务器计算机上运行。

10.4.1 启动 IIS 4.0 的 Internet 服务管理器

Microsoft 管理控制台 MMC(Microsoft management consol)是 IIS 4.0 的主要管理界面,它提供了一个容纳各种管理工具的标准框架,管理员可以按照自己的习惯制定具有个性色彩的管理界面。IIS 4.0 的 Internet 服务管理器的启动方法如下:

在 Windows NT 任务栏上,依次选择"开始"→"程序(P)"→Windows NT 4.0 Option Pack→Microsoft Internet Information Server→"Internet 服务管理器"命令选项,进入 MMC 的界面,稍候,自动激活如图 10-14 所示的窗口。

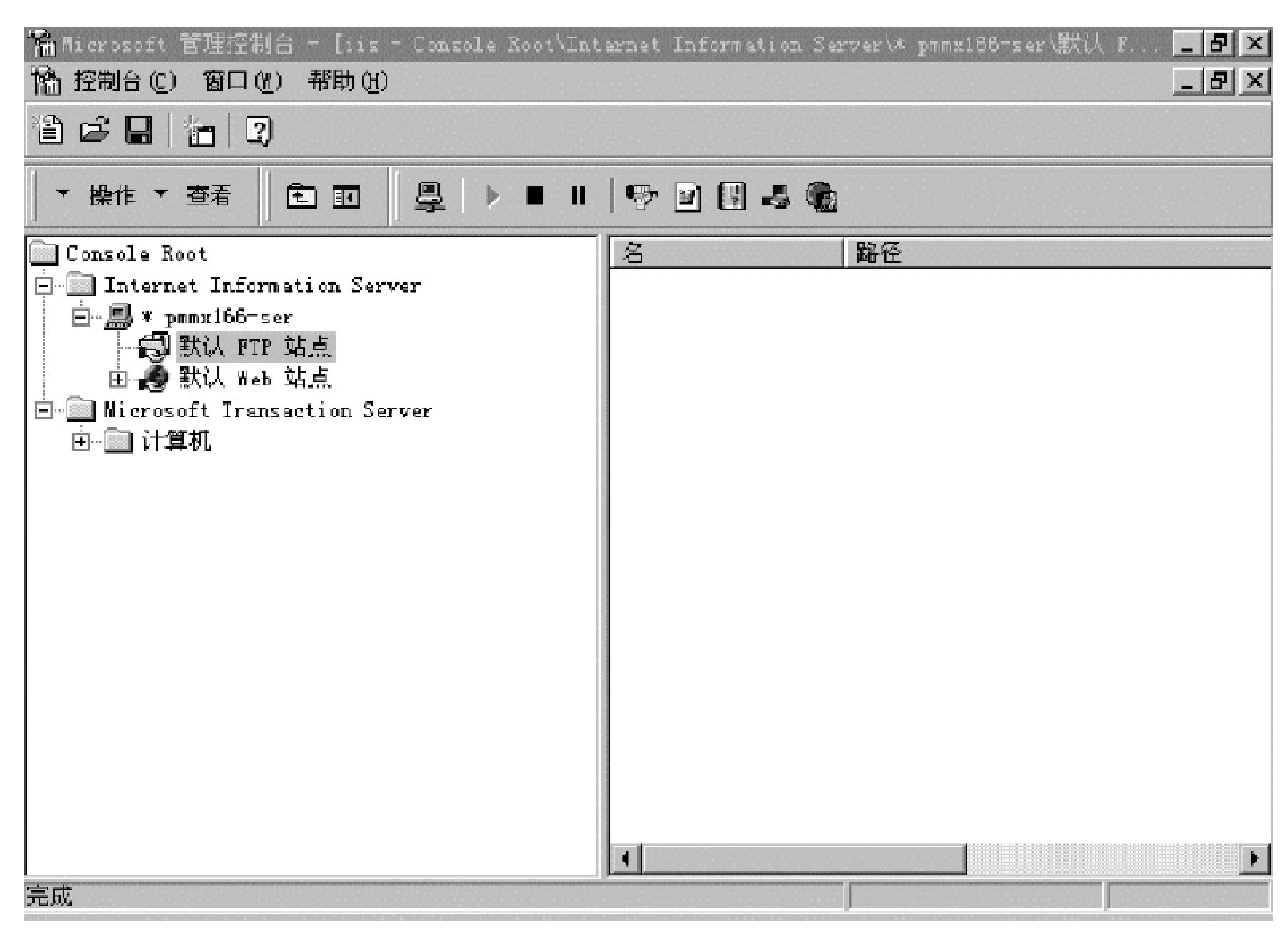


图 10-14 IIS 4.0 的"Microsoft 管理控制台"窗口

10.4.2 配置 IIS 4.0 的 WWW 服务

下面对 IIS 4.0 中有关 WWW 服务的设置和管理步骤作简要的介绍。

① 如果用户需要更改或新增 Web 站点,可以在图 10-15 中,选中"默认 Web 站点",单击鼠标右键,在激活的快捷菜单中选择"属性"命令,即可对选中站点的属性进行修改。

如果不作修改，就可以使用默认的目录路径发表自己的主页。

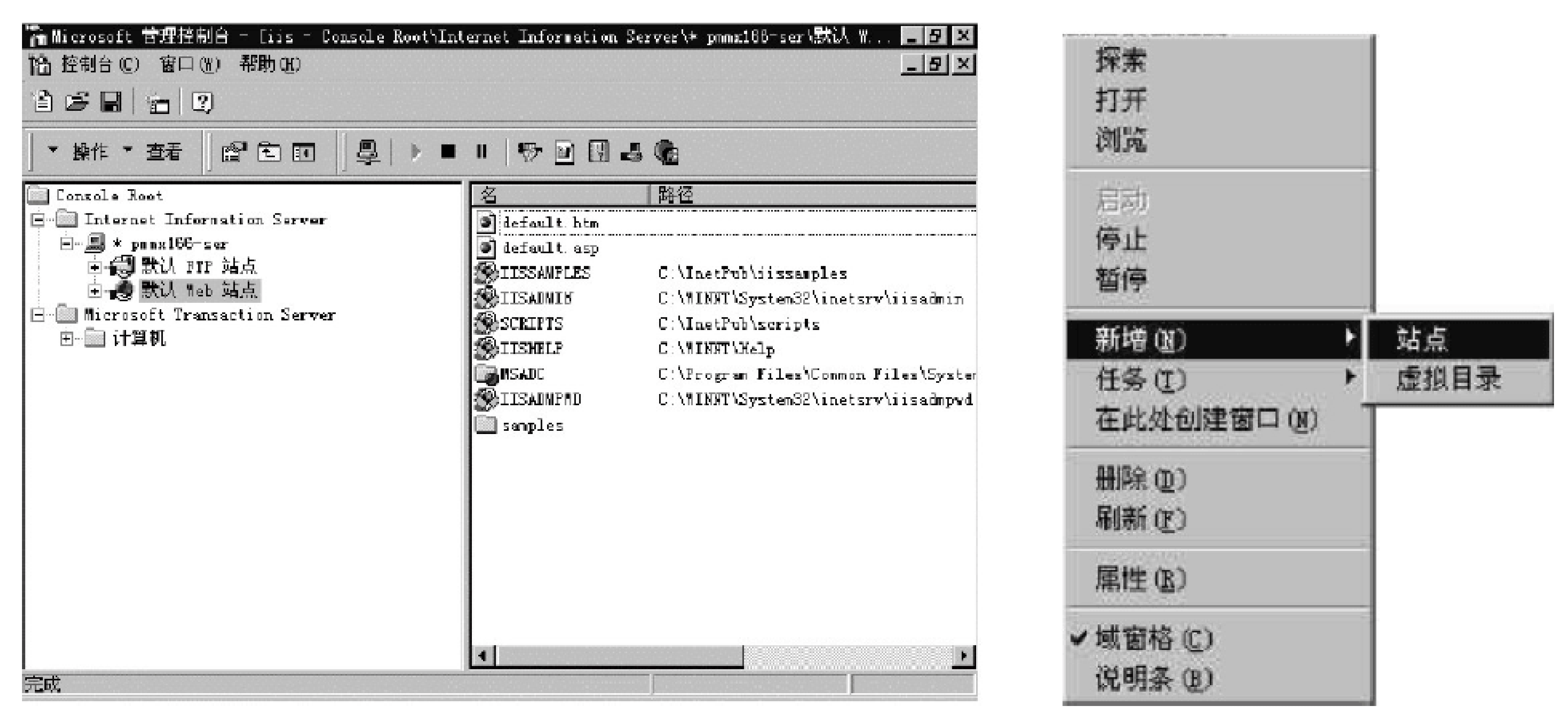


图 10-15　IIS 4.0 的“Microsoft 管理控制台”与“默认 Web 站点”处的快捷菜单窗口

② 安装和配置 WWW 服务器之后，即可将自己所编制的主页发布到指定位置，例如：将自己的主页 default.htm 复制(发布)到默认的路径 C:\InnetPub\wwwroot 处，应注意使用系统默认文档的名称，如 default.htm。

③ 配置之后，在服务器和客户机上，即可使用 IE 浏览器访问刚刚建立的 WWW 服务器，以测试刚刚发布的主页和 WWW 服务器的工作。

注意：在图 10-15 中，选择“默认 Web 站点→属性”可对默认路径和文档进行修改。

10.4.3　NT 客户机访问 WWW 服务器时的设置

NT 网络中的 NT Server 和 NT Workstation 访问 WWW 服务器的主页之前，应当对其安装的 TCP/IP 协议作必要的设置，否则不能正常使用域名对其进行访问。

1. 在局域网内 NT 客户机访问 WWW 服务器时的设置

在局域网内 NT 客户机(指安装了 NT Server 和 NT Workstation 的计算机)访问 WWW 服务器时的设置步骤如下：

① 在“控制面板”中打开“网络”窗口，选择“协议”选项卡。

② 在激活的如图 10-12 所示的“协议”选项卡中，选择“TCP/IP 通信协议”，单击“属性”按钮，激活如图 10-13 所示的窗口。

③ 在图 10-13 所示的窗口中，选择“DNS”选项卡，需要对该客户机的主机名称和 DNS 域名等进行设置，设置说明如下所述：

- 主机名　输入客户机本身的计算机名称。
- 域　输入 DNS 服务器创建的域名。
- DNS 服务器搜索顺序　添加 DNS 服务器所使用的 IP 地址。

④ 完成之后，单击“确定”按钮，重新启动计算机。至此，有关 NT 客户机的 DNS 相关的基本设置完成，如果需要对上述参数进行修改，可以打开对应的窗口进行更改。

⑤ 启动 IE 或其他浏览器。

⑥ 在 IE 浏览器的 URL(统一资源定位器)后的地址栏输入用户主页的 IP 地址或域

名，即可浏览到如图 10-16 所示的用户刚刚发布的主页。



图 10-16　浏览器中访问发布的用户主页

2. 远程访问 WWW 服务器上的用户主页

在局域网内设置好远程访问服务器后，可以使用 NT 计算机对该主页进行远程访问。远程客户端的设置步骤如下：

① 设置好远程工作站的各种协议、与远程访问相关的各种参数，以及客户机对局域网的拨号访问权限。

② 使用远程拨号网络，呼叫局域网内的远程访问服务器的电话号码，直至连接成功。

③ 启动客户端的 IE 或其他浏览器。

④ 输入用户欲访问主页的 URL 地址，即可浏览用户发布的主页，如图 10-16 所示。

10.4.4　Windows 98 客户机访问 WWW 服务器时的设置

NT 网络中的 Windows 95/98 工作站在访问 WWW 服务器的主页之前，也必须对其安装的 TCP/IP 协议作必要的设置，否则也不能使用域名对其进行访问。

在局域网内的设置和访问步骤如下：

① 在 Windows95/98 工作站上，依次选择“开始”→“设置”→“控制面板”命令选项。

② 在打开的“控制面板”窗口中，双击“网络”图标，激活如图 10-17 所示窗口。

③ 在图 10-17 所示的窗口中，选择该计算机网卡所对应的 TCP/IP 协议后，单击“属性”按钮，激活如图 10-18 所示的窗口。

④ 在图 10-18 所示的窗口中，选择“DNS 配置”选项卡，并对其进行配置。配置的内容与 NT 客户机类似，用户可以参照进行。

⑤ 启动 IE 或其他浏览器。

⑥ 在 IE 浏览器的 URL(统一资源定位器)后的地址栏输入用户主页的 IP 地址或域名，即可浏览到如图 10-16 所示的用户刚刚发布的主页。

至此，服务器与客户机端的有关设置已经完成，如果用户打开本机或者任意一台已设



图 10-17　Windows 98“网络”窗口

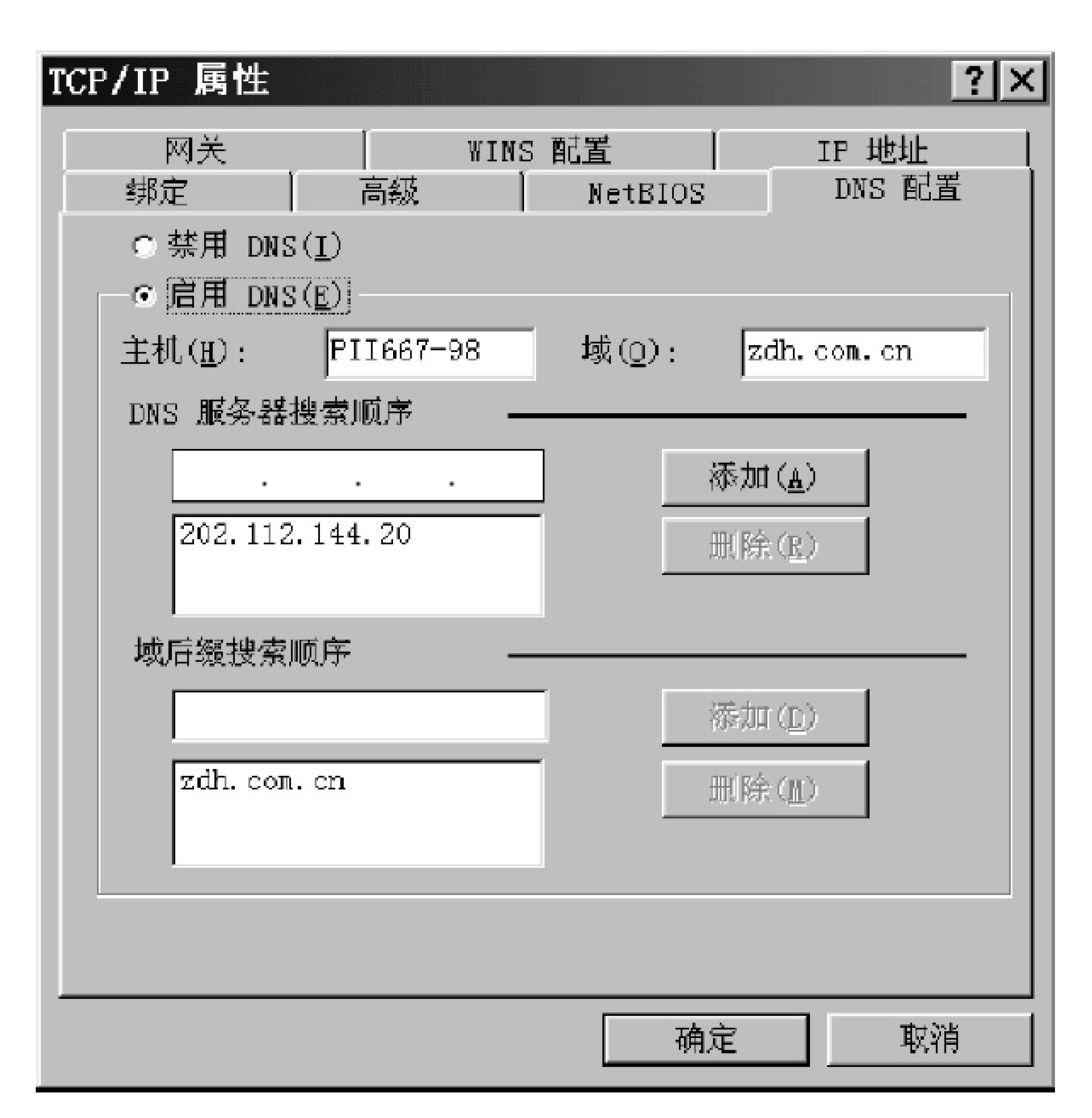


图 10-18　Microsoft TCP/IP 属性的“DNS 配置”选项卡

置好的网络客户机的 IE 浏览器，在 URL 栏输入以下几种许可的地址，进行检测，均应该可以看到 IIS 4.0 默认的主页。

- 服务器端　输入“http://127.0.0.1”。
- 服务器端　输入本机的 IP 地址“http://202.112.144.20”。
- 服务器端　输入本机的计算机名“http://pmmx166-ser”。
- 服务器端　输入本机的域名“http://zdh.com.cn”。
- 客户机端(Windows 98/NT)　输入服务器端的 IP 地址“http://202.112.144.20”。

- 客户机端(Windows 98/NT)　输入服务器端的域名“http://zdh.com.cn”。
- 客户机端(Windows 98)　输入服务器端的计算机名“http://pmmx166-ser”。

10.4.5 配置 IIS 4.0 的 FTP 服务器

本小节介绍配置 IIS 4.0 的 FTP 服务的方法与步骤。

① 在图 10-19 所示的窗口中,如果用户需要更改或设置 FTP 站点,应先选中该站点,例如:“默认 FTP 站点”,单击鼠标右键,在激活的如图 10-19 中所示的快捷菜单中选择“属性”命令,激活图 10-20 所示的窗口,即可对选中站点的属性进行修改。如果不作修改,就可以使用默认的目录路径,向用户提供系统的共享文件和目录等资源。

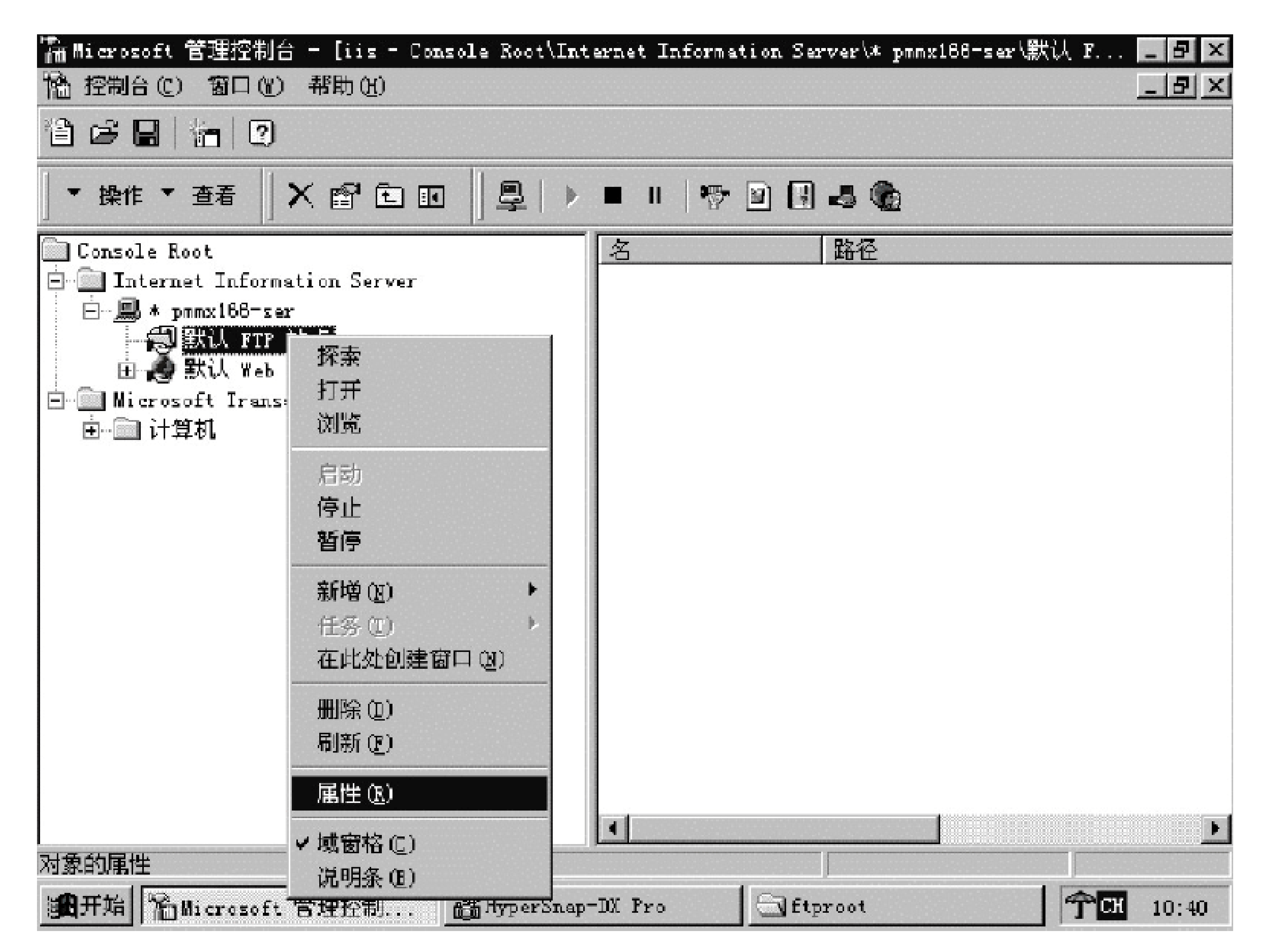


图 10-19　IIS 4.0 的“Microsoft 管理控制台”与“默认 FTP 站点”处的快捷菜单窗口

② 在图 10-20 所示窗口的“FTP 站点”选项卡中,可以对选中站点的属性进行修改,对于初学者建议使用此选项卡所示的系统默认值。之后,在窗口中选择“信息”选项卡,激活如图 10-21 所示的窗口。

③ 在图 10-21 所示的“信息”选项卡中,可以输入用户访问此站点时的欢迎信息和退出信息。然后,在窗口中选择“安全帐(账)号”选项卡,激活如图 10-22 所示的窗口。

④ 在图 10-22 所示的“安全帐(账)号”选项卡窗口中,如果去掉“只允许匿名连接”前的对勾,则表示用户不但可以用“匿名”方式登录 FTP 服务器,还可以进行非匿名方式的访问。例如,在该图中可以添加一些账户和组,以便用户使用域中有效的账户,以非匿名方式登录 FTP 服务器。选择之后,将激活图 10-23 所示的窗口。

注意:

- 默认的登录方式为“匿名”登录方式。即登录 FTP 服务器时,使用 anonymous 作为用户名,使用合法的 E-mail 地址(如 shang@hotmail.com)作为用户密码进行登录。



图 10-20 “默认 FTP 站点 属性”的“FTP 站点”选项卡

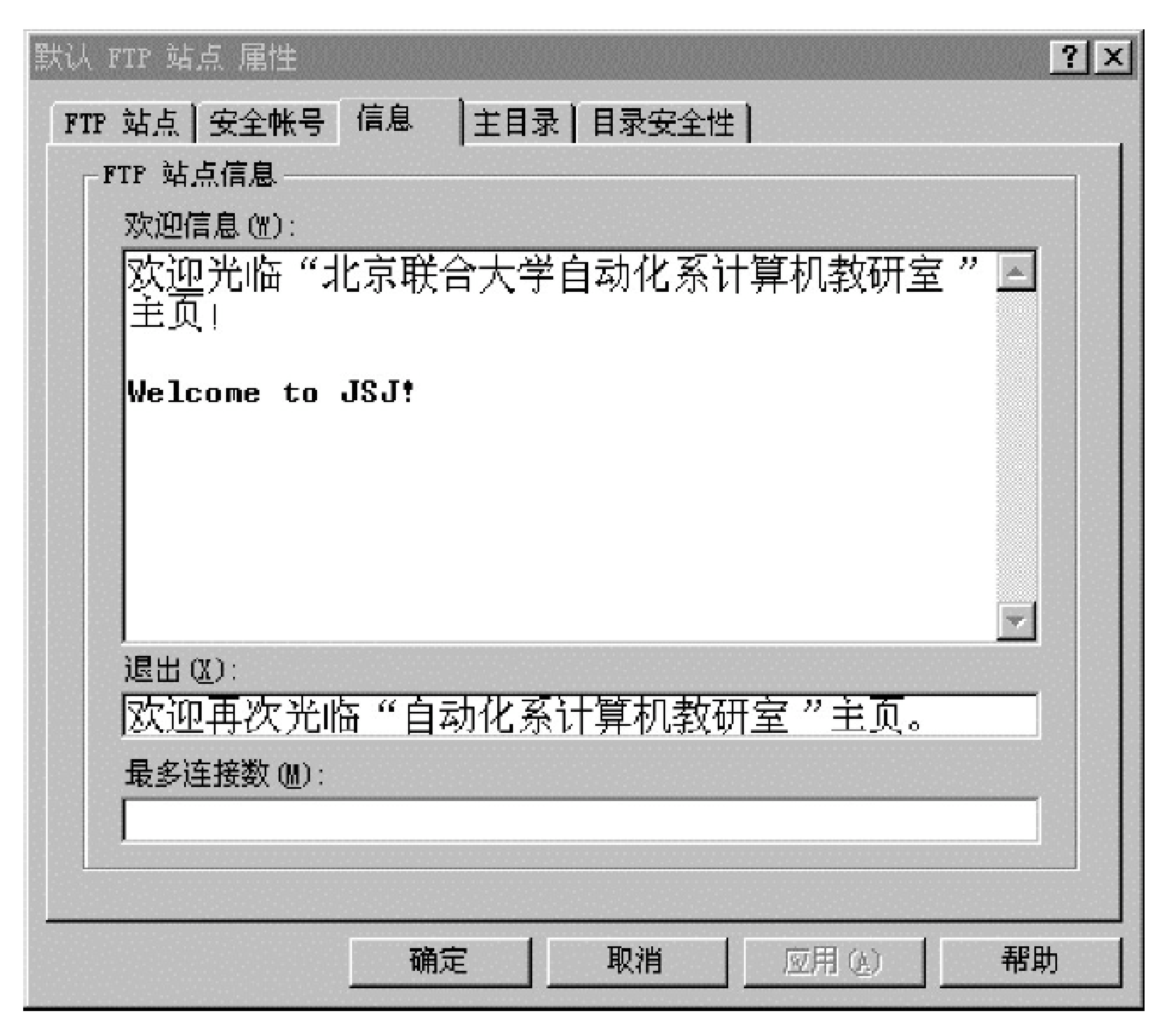


图 10-21 “默认 FTP 站点 属性”的“信息”选项卡

• 在图 10-22 所示的窗口中,如果去掉“允许匿名连接”前的对勾,则表示只允许有效账号的登录方式。

⑤ 在图 10-23 所示的窗口中进行选择后,返回图 10-22 所示的窗口。例如,选择单击“是”按钮。

⑥ 在图 10-22 所示的窗口中,单击“添加”按钮,激活如图 10-24 所示的窗口。

⑦ 在图 10-24 所示的窗口中,从上边的“名称”列表中,选择可以登录 FTP 服务器的用户账号和组账号。选择之后,单击中部的“添加”按钮将选中的账户加入到“添加名称”列表中,最后,单击“确定”按钮,返回图 10-22 所示的窗口。

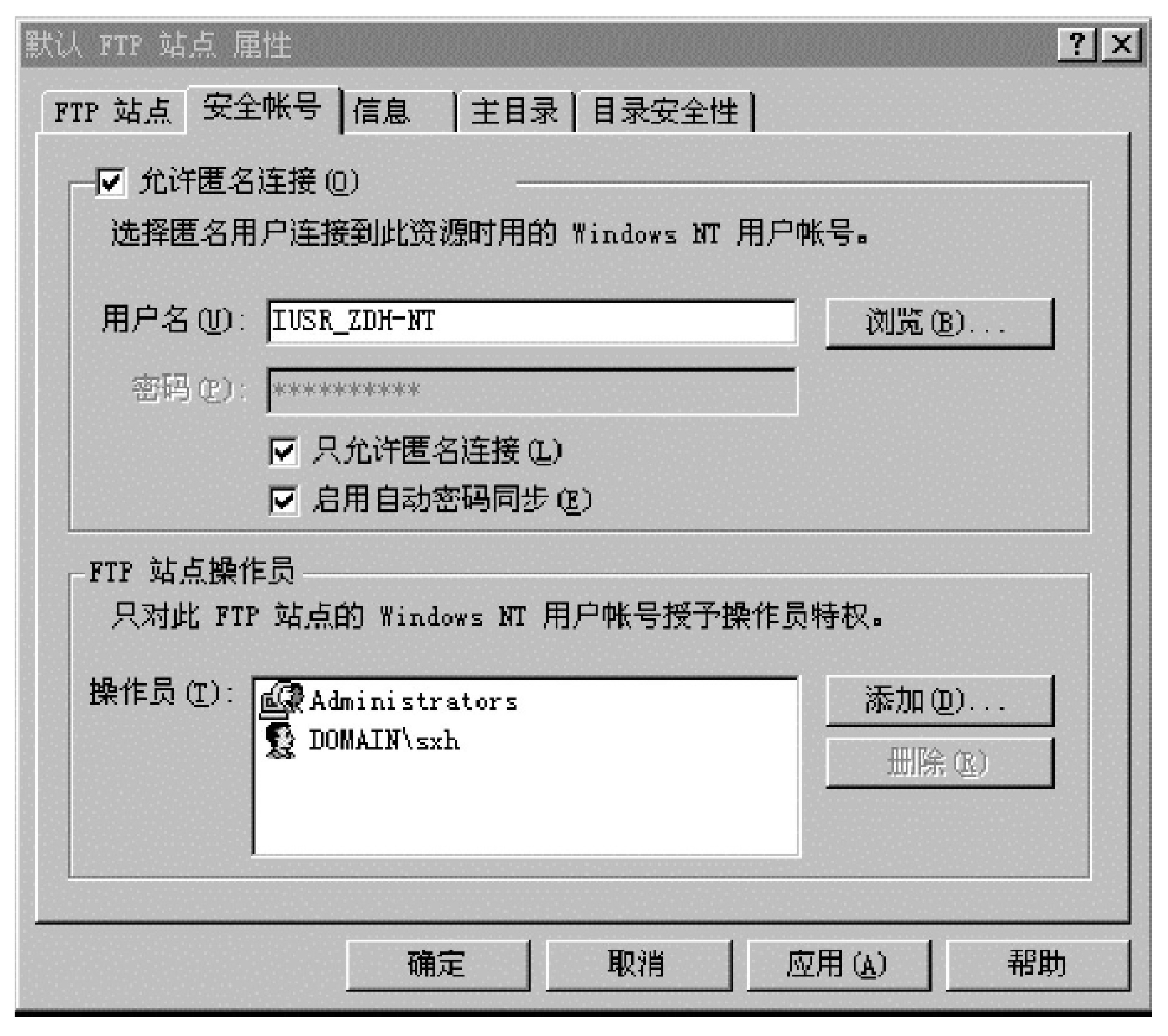


图 10-22 “默认 FTP 站点 属性”选项卡

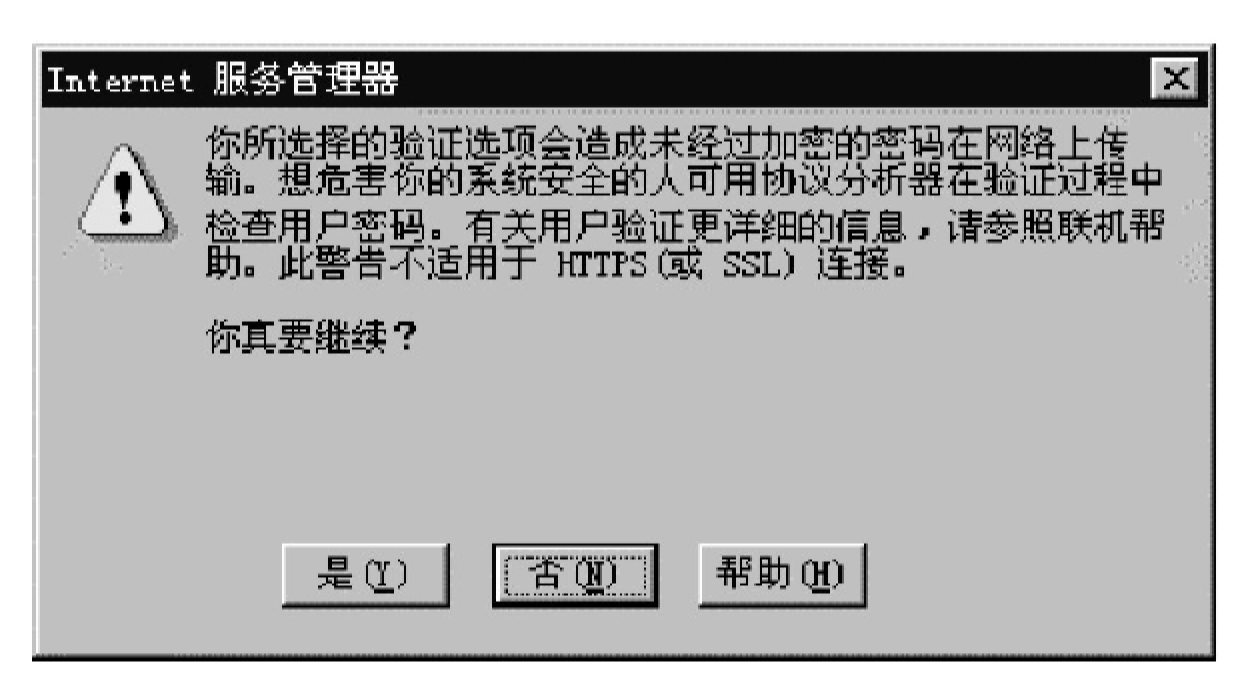


图 10-23 “Internet 服务管理器”的安全选择对话框



图 10-24 “添加用户和组”窗口

⑧ 在图 10-22 所示的窗口中,单击“确定”按钮,完成允许有效账号的登录设置工作。

⑨ 安装和配置 FTP 服务器之后,即可将需要提供给用户共享的各种应用软件和程序复制到指定位置,例如,发布到默认的路径 C:\InnetPub\ftproot 处。

⑩ 配置之后,在服务器和客户机上,即可使用 IE 浏览器访问刚刚建立的 FTP 服务器,以测试刚刚提供的各种程序和 FTP 服务器的工作。

10.4.6 各种客户机对 FTP 服务器的访问

在 NT 网络中,NT 客户机和 Windows 98 客户机在访问 FTP 服务器的主页之前,都必须先对其安装的 TCP/IP 协议做必要的设置,否则不能使用域名对服务器中的资源进行访问。

1. 在 DOS 环境下匿名登录 FTP 服务器

在 DOS 环境下匿名登录和访问 FTP 服务器的步骤如下:

① 依次选择“开始”→“运行”命令选项,激活“运行”窗口。在该窗口中,输入调用 FTP 程序的命令“ftp ftp.zdh.com.cn”后,单击“确定”按钮,激活如图 10-25 所示的窗口。如果在 MS-DOS 方式下输入,也可以激活该窗口。

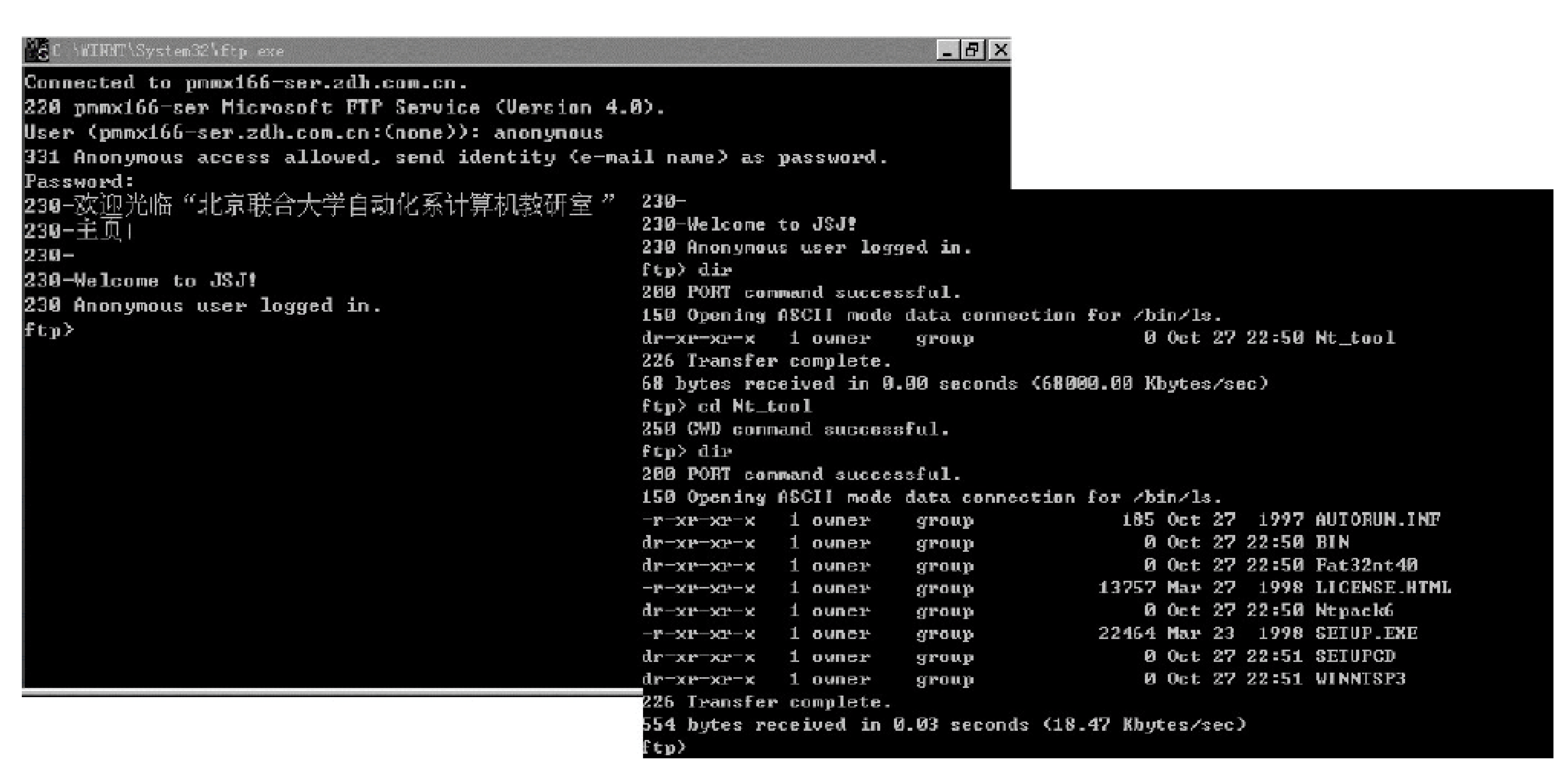


图 10-25　运行“FTP”程序后的 DOS 窗口

② 在图 10-25 所示的窗口中,输入 FTP 服务器匿名登录的账户名,即输入 anonymous 作为用户名,输入用户合法的 E-mail 地址(如,shang@hotmail.com)作为用户密码进行登录,成功后的提示信息如图 10-25 窗口所示。

说明:登录成功后用户可以使用“dir”、“?”和“cd”等 DOS 命令,就可以使用 FTP 服务器提供的资源了。

2. 在 Windows 环境下非匿名方式登录 FTP 服务器

在 IE 中,使用 FTP 服务器允许使用的用户账号登录和访问 FTP 中的资源的步骤如下:

① 在 Windows 环境下打开 IE 浏览器,在“地址”中输入 FTP 服务器资源地址,例如“ftp:// ftp.zdh.com.cn”,按 Enter 键,激活如图 10-26 所示的窗口。



图 10-26　在 IE 浏览器中输入 URL 地址后的账户输入窗口

② 在图 10-26 所示的“登录”对话框中，输入在 FTP 服务器上有效的用户账号和密码。登录成功后，激活如图 10-27 所示的窗口。

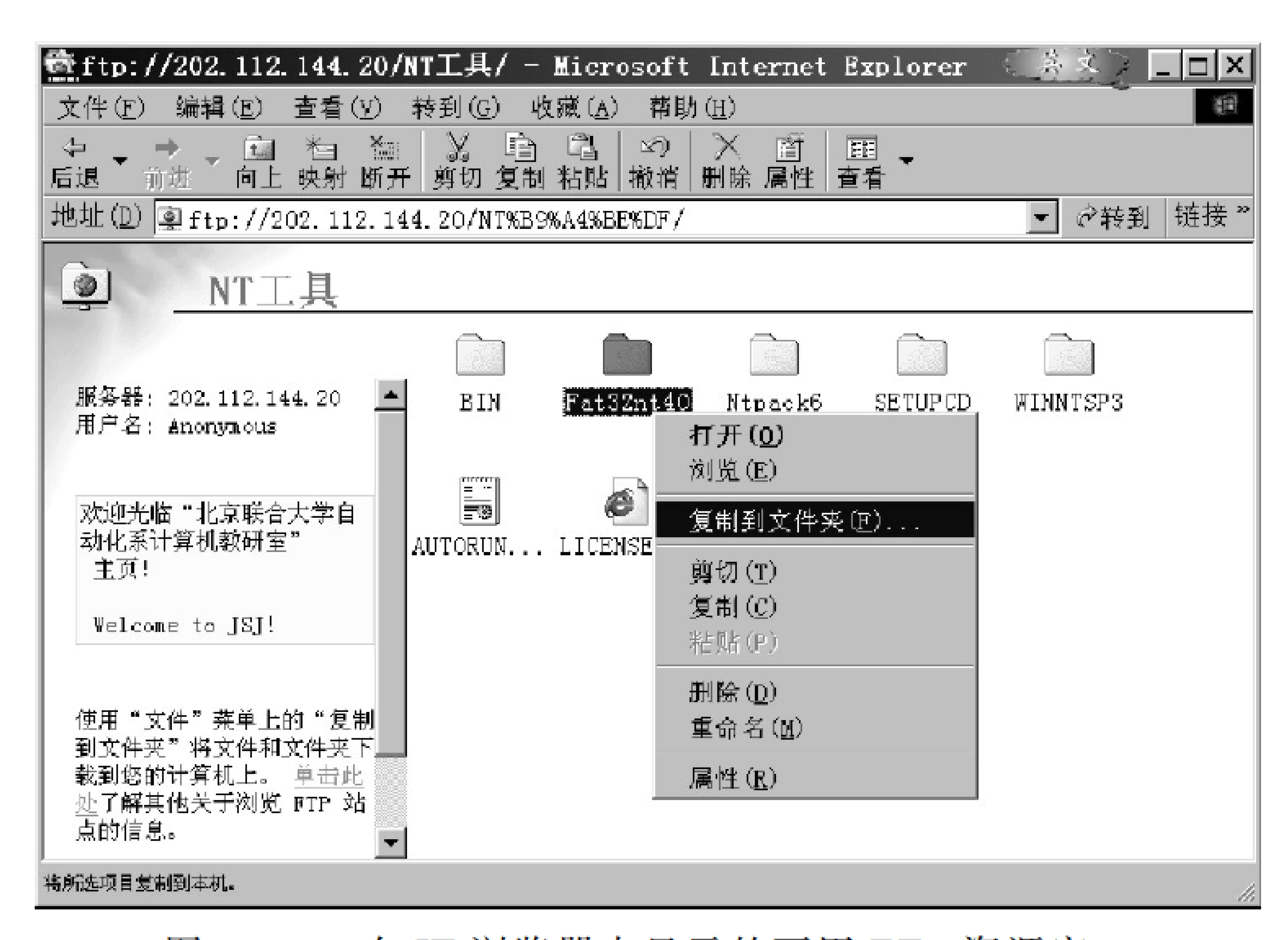


图 10-27　在 IE 浏览器中显示的可用 FTP 资源窗口

③ 在图 10-27 所示的浏览器窗口中，选中 FTP 服务器上的资源后单击鼠标右键，激活快捷菜单。

④ 在图 10-27 所示的“快捷菜单”中，选择使用资源的方式，例如，选择“复制到文件夹”，可以将选中的资源复制到用户选择的文件夹中。

说明：用户也可以使用专用的 FTP 客户端软件，例如 CuteFTP、WS_FTP 等，访问 FTP 服务器的资源，使用方法与在 Internet 中使用时一致。

习题

（1）IIS 2.0/3.0/4.0 各有什么特点？应如何安装 IIS 4.0？
（2）什么是虚拟主机技术？它有什么作用？
（3）安装 Windows NT "Internet 服务器"的主要步骤有哪些？
（4）Internet 服务器管理器的功能有哪些？
（5）什么是 DNS？使用它有什么用处？
（6）如何安装 DNS 服务器 ？如何配置 DNS 的客户机？
（7）如何使用 DNS 管理器？它有什么功能？
（8）如何建立 WWW 服务器？
（9）如何在 WWW 服务器上发布用户主页？
（10）如何在 Windows NT 客户机上访问用户的主页？客户端的主要设置有哪些？
（11）如何在 Windows 98 客户机上访问用户的主页？客户端的主要设置有哪些？
（12）如何建立和配置 FTP 服务器？
（13）如何在 FTP 服务器上提供共享软件？
（14）什么是匿名登录？什么是非匿名方式账户登录？登录时的信息有哪些？
（15）如何实现非匿名登录？服务器端和主要的客户端设置有哪些？
（16）如何在 Windows NT 客户机上访问用户 FTP 资源？客户端的主要设置有哪些？
（17）如何在 Windows 98 客户机上访问用户 FTP 资源？客户端的主要设置有哪些？

实训题目

1. Windows NT IIS 的安装(IIS 2.0 和 IIS 4.0)。
2. Internet 服务器的管理和设置(IIS 2.0 和 IIS 4.0)。
3. DNS 服务器的安装、设置和管理(IIS 2.0 和 IIS 4.0)。
4. WWW 服务器的安装和设置(IIS 2.0 和 IIS 4.0)。
5. 访问局域网内的 WWW 服务器(IIS 2.0 和 IIS 4.0)。
6. FTP 服务器的安装和设置(IIS 2.0 和 IIS 4.0)。
7. 匿名方式登录访问 FTP 服务器的设置(IIS 2.0 和 IIS 4.0)。
8. 非匿名方式(即使用创建的用户账户)登录和访问 FTP 服务器时的设置(IIS 4.0)。
9. DOS 环境下匿名登录和非匿名方式访问局域网内的 FTP 服务器(IIS 2.0 和 IIS 4.0)
10. Windows 98 环境下匿名登录和非匿名方式访问局域网内的 FTP 服务器(IIS 2.0 和 IIS 4.0)。
11. 在远程网络工作站上访问用户的主页和 FTP 服务器的共享资源。

说明：对于没有 IIS 4.0 软件的用户，可以参照书中的步骤，使用 NT Server 中内置的 IIS 2.0 或 IIS 3.0 完成上述实验项目。



第11章 网络的打印管理

本章主要介绍网络管理员应掌握的网络打印服务系统的设计，以及与打印管理有关的基本概念和操作技能。

主要内容：

- NT 网络打印管理的基本概念；
- 网络“打印机”的几种主要连接方式；
- 添加和管理网络打印机；
- 在各种工作站上使用网络打印机打印文件；
- 打印作业的管理；
- 打印过程中常见问题的处理。

11.1 网络打印管理的基本概念

本节将首先介绍网络管理员应当掌握的有关 Windows NT 网络打印服务中所用到的一些基本知识和概念。

11.1.1 网络管理员在打印服务中的基本职责

1. 网络管理员在打印管理中的主要工作

网络管理员在网络打印管理中的主要职责是建立和管理打印服务子系统，主要包括以下几项基本工作职责：

① 选择和设计网络打印设备的连接方式。

② 建立打印服务器。添加和管理网络打印设备。

③ 配置打印工作站。为用户在各种工作站上使用网络打印机做好准备。

④ 打印作业的设置与管理。调整和设置打印机的属性以适应用户的需求。

⑤ 打印中常见问题的处理。

⑥ 打印设备硬件的维护。例如，更换硒鼓和色带，处理打印设备的故障等。

2. 打印服务子系统的建立过程

在网络中，除了文件、文件夹可以共享以外，网络打印机（打印设备）和其他硬件设备

也可以通过网络提供给其他用户使用。网络中提供共享打印功能的设备和方法有两种：第 1 种是“共享打印设备”，即将打印设备接入计算机的普通口，例如 LPT1(并行端口)，并共享该打印设备；第 2 种是“网络打印设备”，在网络中通过内置网卡或者是转换器件可以直接连入网络的打印设备就被称为“网络打印机”，例如，通过网络打印机上的 RJ-45 端口，可以直接连接到集线器或交换机上。这两种方式的设置步骤有所不同，但都较易实现。目前，在中小型单位中应用较多的仍是第 1 种，即利用普通打印设备建立打印服务器。对于这样的用户，若要实现打印机的共享，需要进行如下工作：

① 建立打印服务器　在连有打印设备的计算机上，将与之连接的打印设备设置为共享，使其成为打印服务器。

② 配置打印工作站　在使用共享打印设备的计算机上，设置和指定可使用的“打印机”(已设为共享)的属性，并检测输出的打印文件是否正常。

③ 设置适宜的访问权限。

④ 在微软网络上，不仅 Windows NT 服务器可以充当打印服务器，使其连接的打印机成为共享打印设备，网络工作站也可以完成类似的操作，例如，可以在安装了 NT Workstation 的工作站、Windows 95/98/Me 系统的工作站，甚至 DOS 工作站上都可以连接打印设备，并将它们设为共享状态，供网络上的其他用户使用。它们的设置、使用和管理都很方便。

11.1.2 网络打印管理中的基本术语

1. 打印设备和打印机(printing device & printer)

(1) NT 网络中的打印设备

在 Windows NT 网络中，打印设备就是指产生打印输出结果的实际物理设备。打印设备有两种，一种是连接到打印服务器本地打印端口上的普通打印设备；另一种是带有网络接口(如 RJ-45)的网络打印设备，它可以直接连接到网络上而不必连接到打印服务器的打印端口上。

(2) NT 网络中的打印机

需要注意的是，在 Windows NT 网络中，“打印机”不是指一般物理概念上的打印机，而只是一种逻辑上的打印机，它是应用程序与“打印设备”之间的软件接口，网络用户打印时正是通过这个接口完成打印操作的。与通常的打印机一样，每一个这样的打印机都作为一个单独的窗口出现，并且可以使用“打印机”窗口对其进行管理。

(3) 在 NT 网络中区分打印机和打印设备的目的

正是为了方便用户的使用和管理，在 NT 中才将打印机和打印设备分开。例如，假设某网络系统中有一台打印设备，但是它能以两种形式进行输出，一种以激光效果输出，一种以喷墨效果输出，作为管理员可能对此打印设备的性能非常熟悉，但普通用户可能对此并不了解。在 NT 网络中，网络管理员可以为该打印设备创建两台打印机，每台打印机分别使用不同的打印驱动程序，一台以激光模式输出，一台以喷墨效果输出。用户只需根据自己的需要将打印作业输出到相应的打印机上即可。这样对于同一台物理打印设备，通过将它设置为不同的打印机，并分别为每个打印机指定不同的优先级别和特定的打印时

间，从而实现不同用户对同一打印设备的优先级别、时段和权限控制等特殊的需求。

2. 打印服务器(print server)和打印客户机(print client)

(1) 打印服务器

在网络中，打印服务器是指提供网络打印设备和打印服务的计算机，通常是一台或多台连接了打印设备的计算机或专用设备。由于一台计算机上的打印端口数量和类型都有限，因此，如果需要可以在市场上选择配置有多个打印端口的专用打印服务器，价格在2 000～4 000元左右，例如，某打印服务器具有一个RJ-45端口、一个BNC端口和3个并行端口(LPT)，可以用来连接10base-T、10base-2网络和3台具有并行端口的打印设备。

当打印工作量很大时，如果使用“主域控制器”或“客户机”连接打印设备，将降低它们的工作效率。因此，在实际中通常需要使用一台专门的计算机或设备处理网络上的打印工作，这台专门用于打印管理的计算机就叫做“打印服务器”。一般充当“打印服务器”的计算机至少应配置32MB以上的内存，它还应当与物理打印设备直接连接，并且安装了该设备的打印驱动程序。

(2) 打印客户机或工作站

在网络中，使用网络打印设备和打印服务的计算机均可称为打印客户机或工作站。

3. 打印驱动器

打印驱动器是应用程序和打印设备互相通信的软件接口。它产生组成打印作业的数据流。

4. 打印机和打印队列(printer & print queue)

在许多网络环境中，一般会用到“打印队列”(print queue)这一术语，而在NT中使用“打印机”代替了“打印队列”。例如，在Windows NT中，我们说用户将打印作业提交给打印机，而在OS/2和NetWare中，我们则说用户将打印作业提交给打印队列。在Windows NT中，打印作业被发送给打印机，在它们被送到打印设备之前由假脱机处理程序进行处理。

5. 物理打印端口和逻辑打印端口

根据打印设备的连接位置，通常将打印端口分为物理打印端口和逻辑打印端口两种。

(1) 物理打印端口

物理打印端口是指本地计算机和打印设备之间的硬件接口，例如，Lpt1和com等。

(2) 逻辑打印端口

逻辑打印端口是指本地计算机与远程打印服务器或打印设备的网络连接。例如，在远程打印服务器上创建一个共享打印机，在本地看来就是一个逻辑打印端口，如“\\Server\Printer”。

在Windows NT中，允许在本地创建“打印机”以后使用物理打印端口，或者逻辑打印端口作为打印作业的目的地。

6. 各种打印设备和打印机

(1) 本地打印设备和网络打印设备

本地打印设备指直接与Windows NT工作站或服务器相连的打印设备，它通过共享的方式提供给网络上的用户使用；而网络打印设备则指具有内置网卡或通过转换装置连

接的打印设备，这些设备可以直接与网络相连。例如，通过 hub 或交换机上的 RJ-45 端口连接的打印设备。

(2) 远程打印设备

在 NT 中的远程打印设备就是指可以通过网络，远程访问的打印设备。远程打印设备既可以在本地使用，也可以在远程计算机上使用。

7. 打印机池(printing pool)

(1) 打印机池的定义

打印机池是指通过软件的设置联到一台打印机(printer)上的一组物理打印设备。打印机池的组成见图 11-1。

(2) 建立打印机池的目的

打印机池允许用户将打印文档输出到一台“打印机”上，并由假脱机处理程序来决定输出打印结果的具体打印设备。

打印机池的引入使得网络中的所有打印设备都能得到合理的利用，因而不会出现一台打印设备超负荷运行，而其他打印设备却很空闲的现象。因此，建立打印机池的目的是均衡打印负荷，合理利用打印设备。

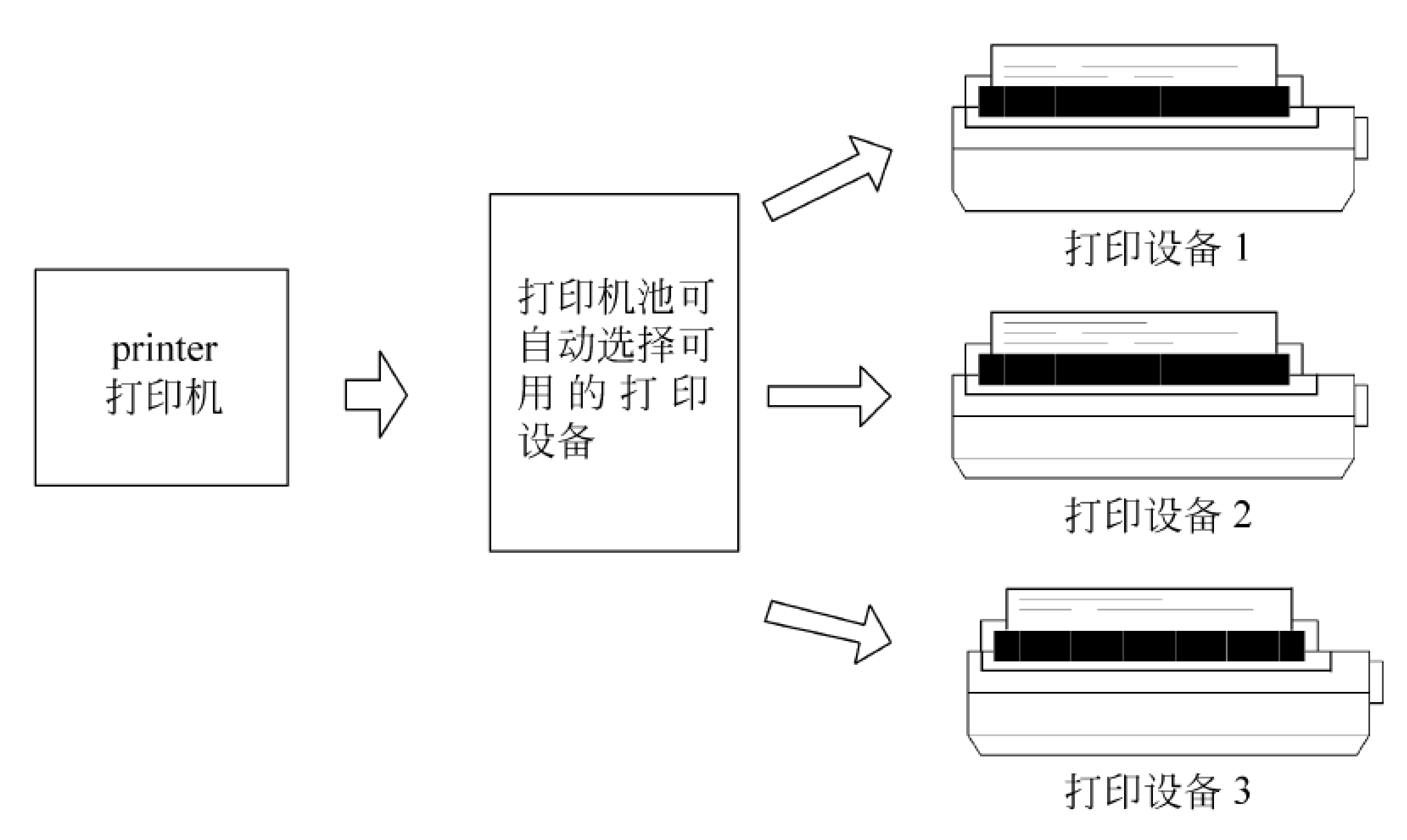


图 11-1　打印机池的组成

(3) “打印机池”的属性

网络管理员若想管理好打印设备，则需建立好打印机池，为此，应当对打印机池具有的属性和特点十分清楚。打印机池具有如下特点：

① 打印机池中的所有打印设备都使用同一个“打印机”，因此它们的属性必须是相同的，即都能使用相同的打印驱动器，例如，使用统一的 Epson LQ-100 ESC/P2 驱动程序。

② 暂停“打印机”，即意味着暂停“打印机池”。因此，暂停“打印机池”这一动作会导致整个“打印机池”所对应的所有物理打印设备都暂停。

③ 所有的打印设备与打印服务器之间，可以通过计算机的串行口(com)、并行口(LPT)，或网络端口与打印设备相连。“打印机池”还可以通过上述各种端口不断扩展规模。

④ 当打印文件送往“打印机池”时，“打印机池”会先检查哪一台打印设备处于空闲状

态，并使该文件通过“空闲”的打印设备输出。“打印机池”检查空闲的顺序为：先安装的端口先检查。例如，先安装的是并行口，就先检查并行口。

⑤ 如果“打印机池”中有一台打印设备因故暂停，则并不影响其他打印设备的使用。例如，一台打印设备卡纸，那么目前正在此打印设备上打印的文件就会被暂停，而其他打印文件还可以由其他打印设备继续打印。

⑥ “打印机池”是通过“打印管理器”在建立“打印机”时，通过为它指定多个输出端口而实现的，并且这些输出端口都连接着具有相同驱动程序的物理打印设备。

8. 打印假脱机

假脱机是打印假脱机处理程序的简称，它是执行打印操作的应用程序与打印监视器之间的接口，它负责将打印作业发送到合适的打印设备。它执行的操作包含以下内容：

① 跟踪打印作业；

② 把作业发送到合适的端口；

③ 跟踪连有打印设备的端口；

④ 为打印作业分配优先级。

9. 打印处理器

打印处理器接收打印作业，并根据数据的类型提供进一步的服务。打印处理器提供的服务主要是把应用程序使用的、描述打印输出的命令，转换成打印设备可以理解的命令，当打印处理器完成了必要的处理之后，就把打印作业返回给假脱机处理程序。

10. 打印监视器

网络操作系统的打印监视器通常负责如下工作：

① 控制流向一个或多个打印端口的数据流；

② 获取对打印端口的访问权利；

③ 往输出目的地写打印作业；

④ 释放对打印端口的访问权利；

⑤ 负责处理不太复杂的错误信息；

⑥ 负责处理真正的结束作业的通知；

⑦ 监视打印机状态，检测打印错误。

11.2 网络打印设备连接方式的设计

在用户使用网络打印设备之前，网络管理员必须合理地组织网络内的打印设备，只有设计合理的打印系统，才能充分发挥出网络打印设备的最大功效。所谓设计网络打印设备的连接方式，实质上就是根据实际情况，设计和选用适宜的网络打印系统方式。

下面将介绍 Windows NT 环境下的“打印机”（逻辑打印机）与“打印设备”（物理打印机）之间的几种配置方式，用户可以根据自身的情况酌情选择和设计自己的打印系统。

1. 一个“打印机”对应一台打印设备

这是最常见和最简单的连接方式，也是目前常使用的方式。

2. 一个“打印机”对应多台打印设备(打印机池)

“一对多”方式是指一个“打印机”名称与多个具有相同功能(即使用同一个打印驱动程序)的打印设备相对应的组织方式。网络管理员可以通过管理一个“打印机”来同时管理和组织多个功能相同的物理打印设备。

当网络上有文件要打印时,“打印机池”会根据打印设备的使用状况来决定由哪台打印设备实施打印。例如,如图 11-1 所示,将 3 台打印设备连接到一台打印服务器的多个物理端口上,“打印服务器”中的“打印机”已被设置为“打印机池”,如果有一个工作站要打印文件,而第 1 和第 3 台打印设备都处于“忙碌”状态,则该打印文件会被自动送往第 2 台打印设备上进行打印。

3. 多个“打印机”对应一台打印设备

“多对一”的方式是指多个“打印机”名称与一个物理打印设备相对应的方式。这种方式可以让 1 台物理打印设备处理由多个“打印机”送来的文件,因此,可以实现对用户优先级和使用时段的分别控制。

下面是 2 个“打印机”对应一台物理打印设备的实例:

实例 1　用户甲使用优先级高的“打印机 1”,用户乙使用优先级低的“打印机 2”。如果用户甲和乙同时打印,则甲的打印文件先输出。

实例 2　用户甲使用的“打印机 1”的时段为 24 小时,而用户乙使用的“打印机 2”的时段为上午 8:00～12:00。如果用户甲和乙同时打印,则用户甲的打印文件可以在任何时间段内输出,而用户乙的文件只能在 8:00～12:00 内输出。

4. 混合方式

这种方式指的是上述几种方式的组合方式,即“一对一”、“一对多”或“多对一”的混合方式。读者可以根据实际需要灵活组织和建立起网络的打印服务子系统。

11.3　打印服务器的建立

建立和管理打印服务器是网络管理员应掌握的主要工作,包括连接打印设备、添加“打印机”、设置网络共享打印机和打印格式等内容。要实现网络打印,首先就要连接物理打印设备,添加“打印机”,并将其设置为共享,最后还要设置好共享访问权限。Windows NT 4.0 提供的“打印机添加向导”可以协助用户完成打印机的安装和设置的大部分工作。

(1) 打印服务器的软件平台

网络管理员应当选择至少一台安装了 NT Server 或 NT Workstation 并连有物理打印设备的计算机作为打印服务器,网络客户将向打印服务器传送打印文档,打印驱动程序应当安装在打印服务器上。

(2) 打印机权限(许可)

① 打印机具有 4 种访问权限:拒绝访问(no access)、打印(print)、管理打印文档(manage documents)和完全控制(full control)。

② 为了保证网络的安全,网络管理员应当为访问某台打印机的用户进行权限的设

置，以限制用户对打印机的访问和操作。在大型公司中，一般将打印机的管理权限分配给一两个特定的用户。上述这些操作都是通过对打印机的权限进行设置来实现的。

(3) 安装与设置打印机的有效账号

网络管理员在安装与设置打印机时，必须使用有效账号登录，登录之后才能完成相应的管理操作。当用户以 administrator 或者是 administrators 身份登录后，可以添加、删除打印机，并且同时具有对打印机完全控制的权限，并能管理打印机。下面是组成员与管理位置的关系：

① administrators　该组成员可以在域中的任意一台运行 NT Server 或 NT Workstation 上对打印机进行管理。

② server operators　该组成员可以在任何一台计算机上管理打印机。

③ print operators　该组成员可以在任何一台计算机上管理打印机。

④ power users　该组成员可以在任何一台存在该组的计算机上管理打印机。

(4) 安装与设置共享打印机的步骤

① 依次选择“开始”→“设置”→“打印机”命令选项，激活图 11-4 所示的窗口。

② 在“打印机”窗口中，单击“添加打印机”图标。

③ 在激活的“「添加打印机」向导”窗口中，选择安装的打印机是“本地打印设备”(即选择“我的电脑”)还是“网络共享打印机”(即选择“网络打印服务器”)，选择之后，单击“下一步(N)”按钮，激活如图 11-2 所示的“「添加打印机」向导”窗口。

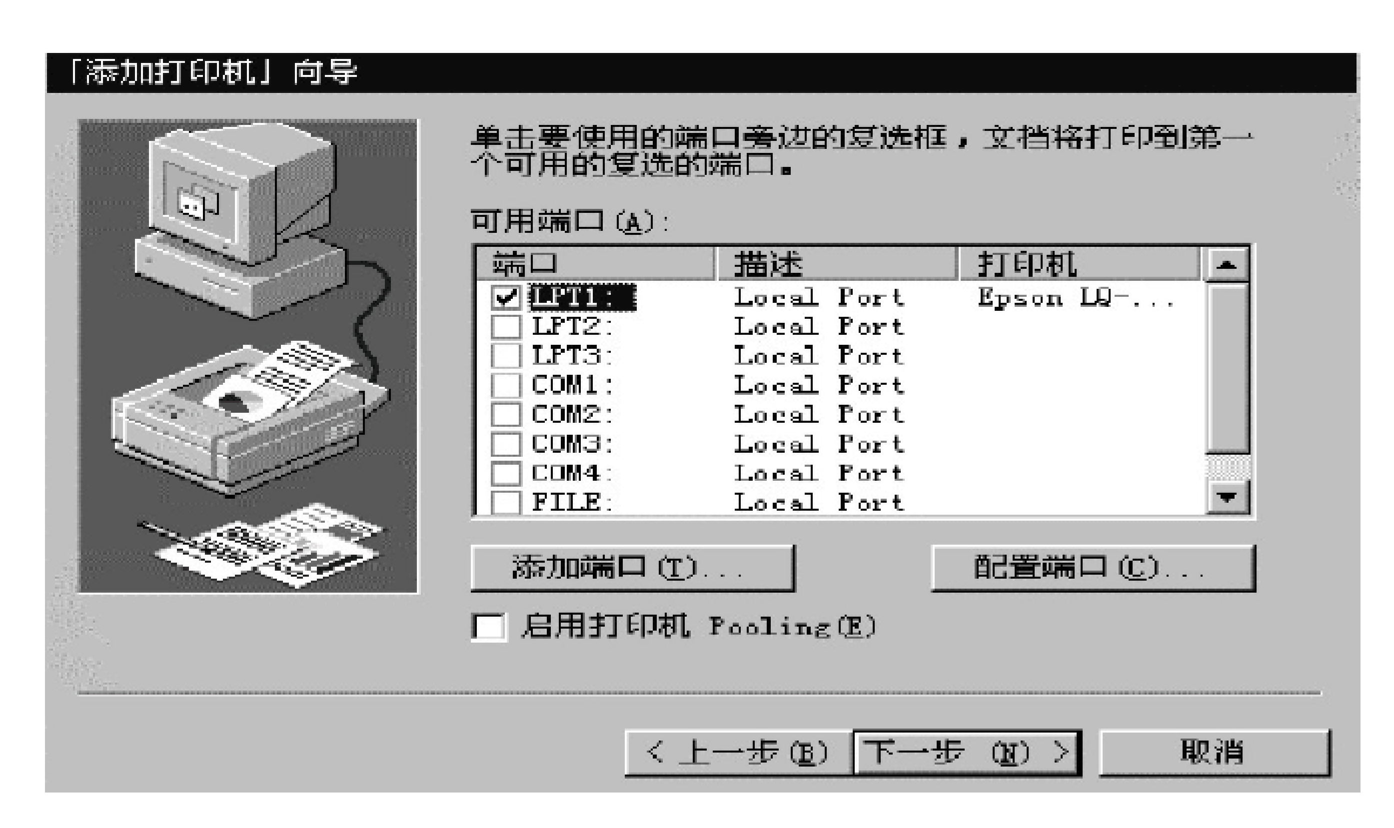


图 11-2 “添加打印机向导”窗口

④ 在图 11-2 所示的窗口中，选择打印设备拟安装的端口，例如，“LPT1”。选择之后，单击“下一步(N)”按钮，激活如图 11-3 所示的后继的“「添加打印机」向导”窗口。

⑤ 在图 11-3 所示的窗口中，选择打印机生产厂商和型号，选择之后，单击“下一步(N)”按钮。

⑥ 在激活的“「添加打印机」向导”窗口中的打印机名称栏中，输入打印机的名称后，单击“下一步(N)”按钮。

⑦ 在后继的“「添加打印机」向导”窗口中，选中“共享”单选项，将网络服务器的打印设备设置为共享打印机。还需键入其共享名称，以供网络上的其他计算机选用。此外，还可以选择安装“Windows 95/98”或“Windows NT...”的打印驱动程序，当使用此类系统的

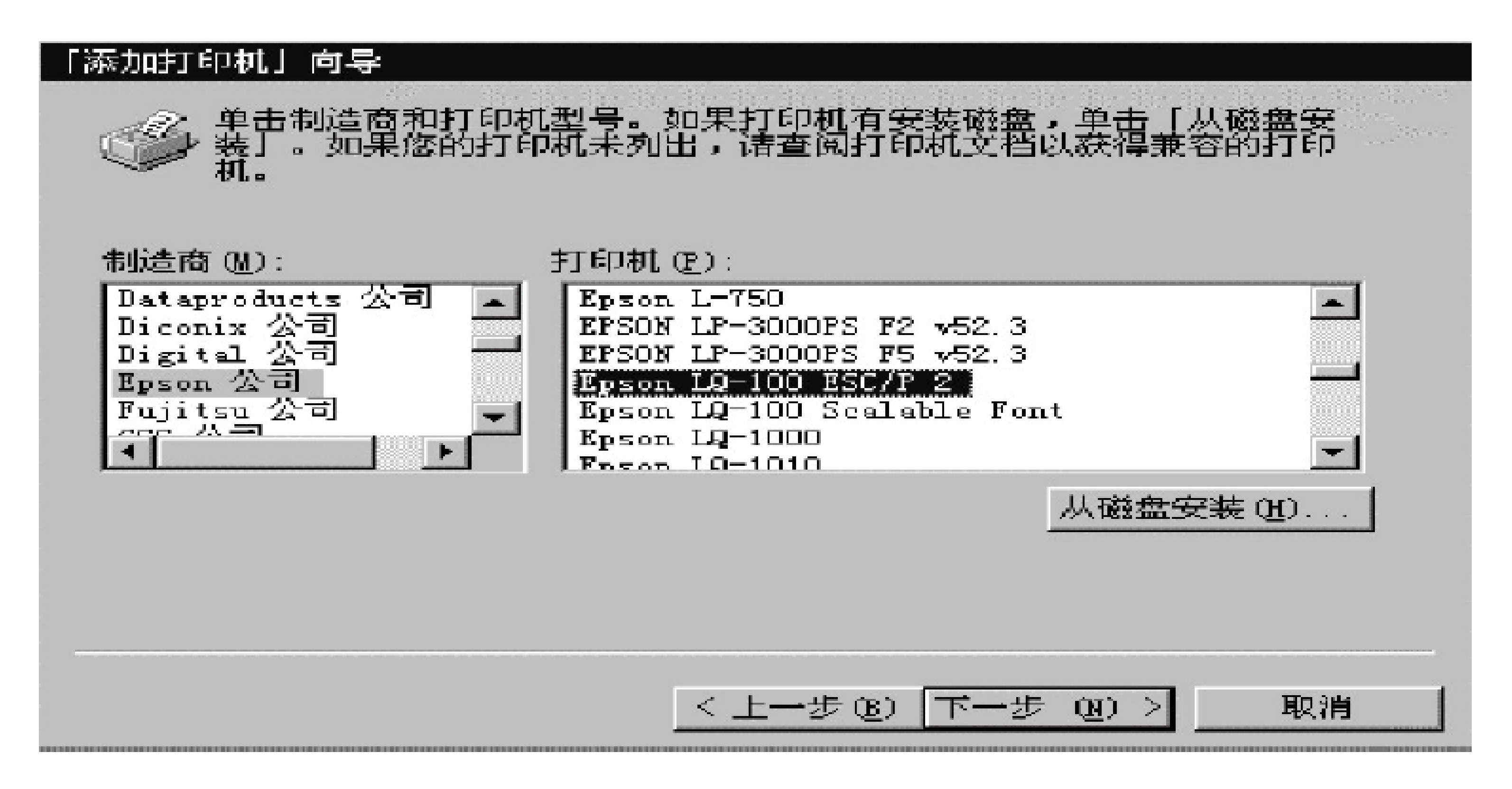


图 11-3 “添加打印机向导”窗口

客户端的计算机连接到共享打印机时，其相应的打印驱动程序就会自动下载到该客户端的计算机中，而无须在客户端以手工方式进行配置。选择之后，单击“下一步(N)”按钮。

⑧ 在激活的后继窗口中，会询问是否打印测试页，以检查打印机的设置是否正确，选择“是”之后，单击“完成”按钮，从打印机上输出一张测试页。

⑨ 由于在步骤⑦中选择了“Windows 95”(98)或“Windows NT...”的打印驱动程序，因此安装向导会要求用户提供相应的软件(或光盘)，以便安装打印驱动程序，用户可根据提示依次安装。打印机安装完毕之后，在图 11-4 所示的“打印机”窗口中，将出现新增的打印机图标，至此，设置打印服务器，即添加网络共享打印设备的操作全部完成。

11.4 打印机的管理

“打印机的管理”是指在打印服务器中对“打印机”属性的管理。因为在添加打印机后，有时用户需要对其参数进行更改。例如，添加打印机时选择的是本地安装方式，以后需要时，又打算将其设为共享；另外，用户还会经常提出管理打印作业的请求。因此，网络管理员除了应当学会如何修改打印机参数外，还应该学会如何管理打印机。打印机的常规管理包括：设置打印机的使用时间段、优先级和改变打印作业的次序等。

11.4.1 “打印机”属性的设置方法

① 依次选择“开始”→“设置”→“打印机”命令选项，激活如图 11-4 所示的窗口。

② 在图 11-4 所示的“打印机”窗口中，选定拟设定属性的“打印机”图标，单击鼠标右键，激活如图 11-5 所示的“打印机”快捷菜单，选择“属性(R)”选项。

③ 在激活的图 11-6 所示的所选打印机的“属性”窗口中，可以根据需要对其中的许多选项卡进行设置。

④ 根据需要选择并设置后，单击“确定”按钮，完成打印机属性的设置。



图 11-4　打印机窗口

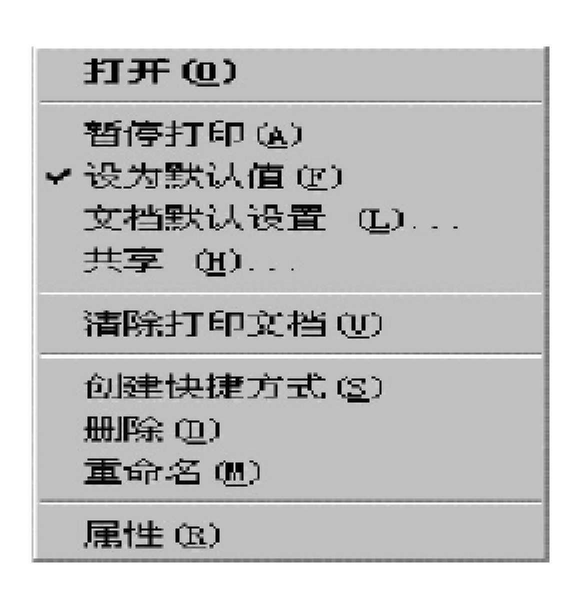


图 11-5　打印机快捷菜单条



图 11-6　打印机属性中的"共享"选项卡

11.4.2　"打印机"属性中的选项卡

1. "常规"选项卡

在所选打印机属性窗口的"常规"选项卡中，包括了打印机属性的许多描述性的设置。例如，打印机名称、备注、位置和使用的驱动程序等。

2. "共享"选项卡

在所选打印机的属性窗口中，选择如图 11-6 所示的"共享"选项卡。与添加打印机时的选择一样，在此处可以对属性进行修改或设置。例如，对是否共享所选的打印机进行设置，若选择"共享"，则应键入共享名称，以及此打印机所支持的计算机操作系统。

3. "调度"选项卡

在图 11-6 所示的窗口中，选择"调度"选项卡，激活如图 11-7 所示的窗口。该窗口可以设置使用此"打印机"的时间段和打印机的优先处理顺序(优先级)等。

① "可用"栏目。在此栏目下，可以设置此"打印机"开始使用与结束使用的时间。默认值为"总是(W)"，表示此打印机每天 24 小时提供服务。

② "优先级"栏目。在此栏目下，可以设置此"打印机"的打印优先级。当多个"打印

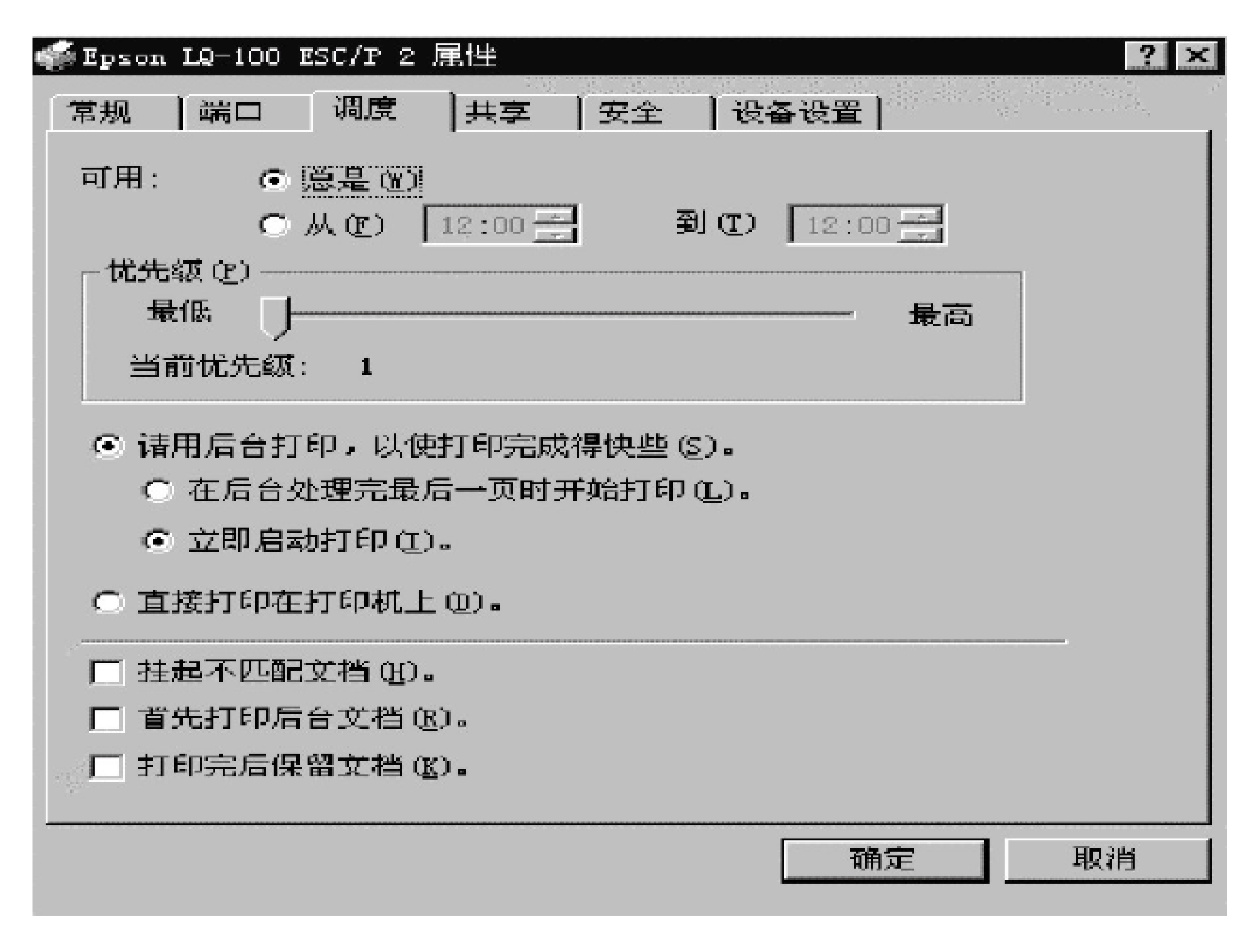


图 11-7　打印机属性中的“调度”选项卡

机”与一台打印设备对应时，例如，服务器上两个“打印机”的共享名称分别为“EpsonLQ-100” 和“EpsonLQ-570”，假定它们都是连接在 Epson LQ-100 ESC/P 2 的打印设备上，如果“Epson LQ-100”的优先级高于“EpsonLQ-570”，则使用“EpsonLQ-100”的打印文件会在打印设备上优先打印。“优先级”栏目的默认值为“1”，这是最低的优先级，最高的优先级为“99”。

③ 选择“请用后台打印，以使打印完成得快些(S)”单选钮，可以先将打印文件保存到硬盘中，然后再将其送往打印设备进行打印。文件送往打印设备的操作是由 spooler(后台缓冲器)在后台执行并完成的。

④ “直接打印在打印机上(D)”单选钮。当用户文件无法使用 spooler 打印(即后台缓冲器无法正常运行)时，可使用这种方式将打印文件直接送往打印设备上。此选项只适合于本机送出的文件，不适合网络客户送来的文件。

4. “安全”选项卡

在所选打印机的属性窗口中，选择“安全”选项卡，激活如图 11-8 所示的窗口。该窗口用于设置所使用“打印机”的安全特性。下页依次介绍该窗口的主要选项：



图 11-8　打印机属性中的“安全”选项卡

① 权限(P)　在上述窗口中,选择"权限(P)"按钮。激活"打印机的权限"窗口,可以进行打印机权限的设置。例如,可设置为不允许访问、打印、管理文档和完全控制。

② 审核(A)　在上述窗口中,单击"审核(A)"按钮,激活"审核 打印机"窗口,在该窗口中,可以选择和添加要审核的用户名单,并设置其需要审核的内容。

③ 所有权(O)　在上述窗口中,单击"所有权(O)"按钮,激活"所有者"窗口,在该窗口中可以查看打印机的所有者。也可以利用"取得所有权(T)"按钮,取得"打印机"的所有权。

11.5　各种网络打印客户机的配置

Windows NT 打印系统的工作模式也是客户机/服务器模式,可以利用 Windows NT 打印服务器上安装的网络共享打印机(网络打印机)进行打印输出的客户机有很多种,例如 DOS 工作站、Windows 95/98/Me 工作站、Windows NT 工作站和服务器以及 Windows 2000 服务器/专业版工作站等。

注意:Windows 95/98/Me 工作站、Windows NT 工作站和服务器都可以直接使用 Windows NT 打印服务器上的打印驱动程序,其他工作站则必须另外安装打印驱动程序。

11.5.1　在 DOS 工作站上使用网络打印机

MS-DOS 应用程序可以提供自己的驱动,以便将数据转换成 RAW,因此,从基于 DOS 的应用程序打印时会跳过 Windows NT 标准打印过程中的一些步骤。

1. 用户可使用的 DOS 命令

① 使用"net use LPTx :\\server\print_share" 命令连接"打印机"。其中,server 为打印服务器的计算机名;print-server 为打印设备的共享名。

由于 DOS 应用程序一般不能理解 UNC(通用命名标准)的命名,所以必须将网络"打印机"映射成物理端口 LPTx,如 LPT1。

② 使用"net use LPTx :/DELETE"命令断开已连接的"打印机"。

③ 还可以使用"NET PRINT"命令管理所打印的文件,例如暂停、删除打印文件等。

从基于 DOS 的应用程序打印时,用户应注意考虑以下的附加条件:

- 如果 DOS 应用程序生成纯文本输出,则不需要特殊的配置。一旦本地连上打印设备,并将该设备设为共享,在应用程序中就可以进行打印。
- 如果 DOS 应用程序打印图形或带格式的文本,则打印程序必须有厂商提供的打印驱动程序,该打印驱动程序应与安装操作系统时使用的驱动程序相同。

2. 在 DOS 工作站使用网络打印机的实例

在 DOS 工作站启动、联接和使用"打印机"的步骤如下:

① 从 DOS 工作站启动"打印机"时,应先登录验证。例如,用户名为 SXH,域名为 ZDHDOMAIN。

② DOS 工作站启动后,若没有自动连接打印机,请使用如下命令连接打印机:

“net use LPTx: \\server\print_share”

例如,对于图 11-9 所示的系统,应键入如下启动“打印机”的命令:

“net use LPT1 \\NT-S-PMMX166\EpsonLQ-100”,成功后即可通过常用的 DOS 打印方式打印需要打印的文件。



图 11-9　DOS 工作站启动网络打印机的命令窗口

③ 打印文件。例如,需要打印 A 盘上的 autoexec.bat 文件。

- 启动 DOS 的文本编辑器,即输入“EDIT A:\AUTOEXEC.BAT”后,按 Enter 键。
- 选择菜单条上的 FILE→Print 命令,即可打印该文件。

11.5.2　在 Windows 95/98 工作站上使用网络打印机

在 Windows 95/98 工作站上使用网络打印机的步骤如下:

1. 添加网络共享打印机

① 依次选择“开始”→“设置”→“打印机”命令选项,激活如图 11-4 所示的“打印机”窗口,从中选择“添加打印机”图标,打开如图 11-10 所示的窗口。



图 11-10　“添加打印机 向导”窗口

② 在图 11-10 所示的“添加打印机向导”窗口中选择“网络打印机(N)”单选钮后,单击“下一步(N)”按钮,激活后继窗口。

③ 在激活的“浏览打印机”窗口中,可以使用鼠标进行浏览,并选定网络打印机,之后,单击“确定”按钮,激活如图 11-11 所示的窗口。

④ 在图 11-11 所示的“添加打印机”向导窗口中,选定网络打印机后,选择是否“从基于 MS-DOS 的程序打印”选项,选择之后,单击 “下一步(N)”按钮,激活后继的窗口。

⑤ 在激活的下一个“添加打印机 向导”窗口中,如果在上一步中,选择了“从基于



图 11-11 "添加打印机 向导"窗口

MS-DOS 的程序打印"选项，则选择并单击"捕获打印机端口(C)"按钮。选择之后单击"下一步(N)"按钮，激活如图 11-12"捕获打印机端口"窗口。否则，跳到步骤⑦。



图 11-12 "捕获打印机端口"窗口

⑥ 在图 11-12 中，选择打印机端口的设备名，选择之后，单击"确定"按钮，激活后继窗口。

⑦ 在激活的后继的"添加打印机 向导"窗口中，输入"网络打印机"名称，并将其设为默认打印机，单击"完成"按钮，激活打印测试窗口。

⑧ 在打印测试窗口中，根据需要选择单选钮"是"或"否"打印"测试页"，若选择了"是"，则打印测试页。

⑨ 在执行⑧之前，应先打开打印设备的电源，放好纸张。稍候将会从此网络共享打印机上输出"Windows 95/98 Printer Test Page(测试页)"。测试过程结束后，出现提示的"测试是否成功"询问对话框窗口，若打印正常，单击"是(Y)"，返回图 11-4 所示的窗口。

⑩ 在图 11-4 的窗口中，可以看到添加了一个新的名为"Epson LQ-570 ESC/P2"的网络共享打印机的图标。

2. 网络共享打印机的使用

网络打印机的设置与连接完成之后，在 Windows 95/98 下使用和管理"打印机"的方法与普通打印设备相同。

11.5.3 在 Windows NT 客户机上使用网络打印机

安装了 Windows NT 的打印客户机有 NT Server 和 NT Workstation，在这些客户机

上使用网络打印机的步骤如下：

1. 添加网络共享打印机

① 依次选择“开始”→“设置”→“打印机”命令选项，激活如图 11-4 的“打印机”窗口，从中选择“添加打印机”图标。

② 在激活的“「添加打印机」向导”窗口中，选择“网络打印服务器(E)”后，单击“下一步(N)”，激活如图 11-13 所示的窗口。

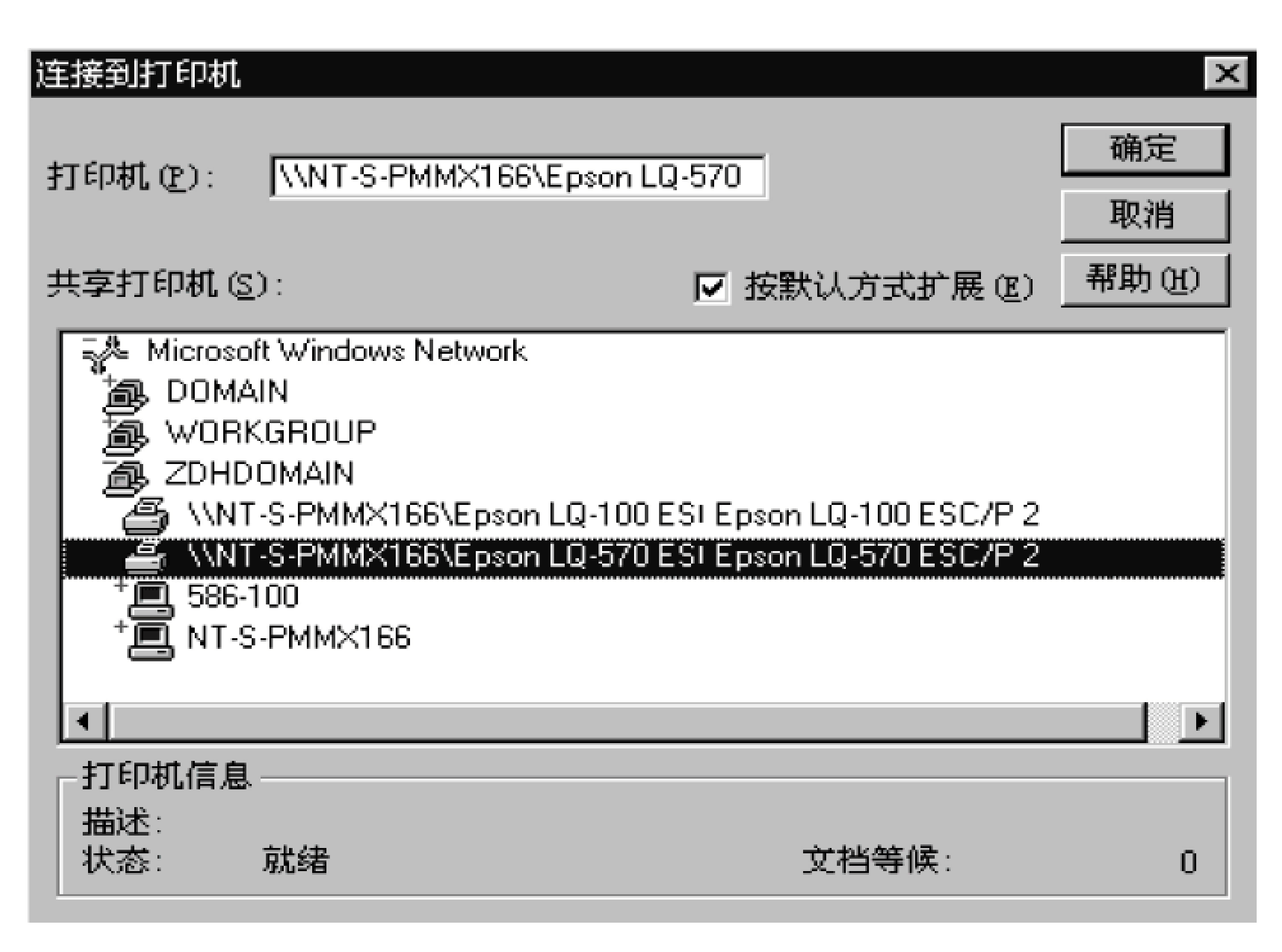


图 11-13 “连接到打印机”窗口

③ 在图 11-13 所示的“连接到打印机”窗口中，浏览并选定网络打印机后，单击“确定”按钮，激活后继的窗口。

④ 在所激活的“添加打印机 向导”窗口中，选择是否将其设为默认打印机，选择之后，单击“下一步(N)”按钮，激活后继的窗口。

⑤ 当出现“网络打印机安装成功”的信息窗口时，表示安装成功，单击窗口中的“完成”按钮，激活与图 11-4 类似的“打印机”窗口。

⑥ 在所激活的“打印机”窗口中，可以看到新添加的名为“Epson LQ-570 ESC/P2”的网络共享打印机的图标。

2. 网络共享打印机的使用

网络打印机设置与连接完成之后，在 Windows NT 下使用和管理“打印机”的方法与普通打印设备相同。

11.6 网络打印服务器的设置与管理

网络打印服务器的管理包含“打印机”的组织与管理及用户打印作业的管理两个方面。

11.6.1 网络中“打印机”的组织与管理

通常网络打印机由许多用户共同使用，有时候，一些用户可能正在打印一些不太紧急

的文件，而另一些用户则需要立即输出打印文件。此时，网络管理员就可以使用“打印机属性”中的“调度”选项卡解决用户的打印优先顺序的问题。

由于无法将不同用户账号设置为不同的优先级，所以可以给同一台打印设备设置两套“打印机”名称，并且把它们均设为“共享”状态；然后，分别设置这两套打印机的优先级，并将它们分配给不同的用户使用。这样，使用优先级高的打印机的打印文件可以优先输出到打印设备上。

1. 设置打印机的使用优先级

① 按上节的方法设置两台网络共享打印机极其共享名，例如，同一台打印设备的“打印机”的共享名分别设置为“EpsonLQ-100”和“EpsonLQ-570”。

② 使用每个“打印机”属性中的“调度”选项卡，分别设置这两台网络共享打印机的优先级。例如，它们的优先级分别为“EpsonLQ-100”的“7”和“EpsonLQ-570”的“1”。

③ 将这两台网络共享“打印机”分别分配给不同的用户。例如，用户 SXH 使用优先级值为“7”的“EpsonLQ-100”打印机，而用户 GZH 使用优先级值为“1”的“Epson LQ-570”打印机，从而满足了在一台物理打印设备上，实现不同用户对打印顺序的不同需求。

2. 设置用户的打印时段

如果网络共享打印机可以在 24 小时内使用，通过上述方法还可以给不同用户分配不同的时间使用区段，从而满足用户对同一打印设备的不同使用时段的设置需求。例如，要求用户 SXH 使用打印设备的时段为 08:00～24:00，用户 GZH 的使用时段为 08:00～12:00。由于每台“打印机”只有一个属性选项卡，所以必须先为同一打印设备设置不同的“打印机”名称；然后，为使用不同时段的用户分配不同的“打印机”；最后，通过给每个“打印机”设置不同使用“时段”的方法来满足上述的要求。实现的步骤如下：

① 按上述的方法，将一台物理打印设备设置为两台网络共享“打印机”。例如，对同一物理端口(lpt1)上连接的同一物理打印设备，分别添加两次“打印机”，其名称分别为“EpsonLQ-100”和“EpsonLQ-570”。

② 使用每个“打印机”属性中的“调度”选项卡，分别设置这两个打印机的使用时段。例如，将“EpsonLQ-100”的可用时段设为 08:00～24:00，将“EpsonLQ-570”的可用时段设为 08:00～12:00。

③ 将这两台网络共享的“打印机”分别分配给不同的用户。例如，指定用户 SXH 使用“EpsonLQ-100”打印机；而用户 GZH 使用“EpsonLQ-570”打印机，这样就满足了在一台物理打印设备上，实现不同用户对打印时段的不同设置要求。

11.6.2 打印管理器的管理工作

打印管理工作包括管理“打印机”和管理打印文档两个方面。

1. 启动“打印机”的属性管理窗口

依次选择“开始”→“设置”→“打印机”命令选项，激活如图 11-4 所示的“窗口。在该窗口中，双击需要管理的“打印机”图标，即可打开选定打印机的属性窗口。这个窗口就是“打印机”的管理窗口，例如，如图 11-6 所示的 EpsonLQ-100 ESC/P 2 的属性窗口。

2. 使用打印管理器管理打印文档

(1) 启动打印管理器的步骤

依次选择“开始”→“设置”→“打印机”命令选项，激活如图 11-4 所示的“打印机”窗口，在此窗口中双击要管理的打印机，激活图 11-14 所示的“打印管理器”窗口。

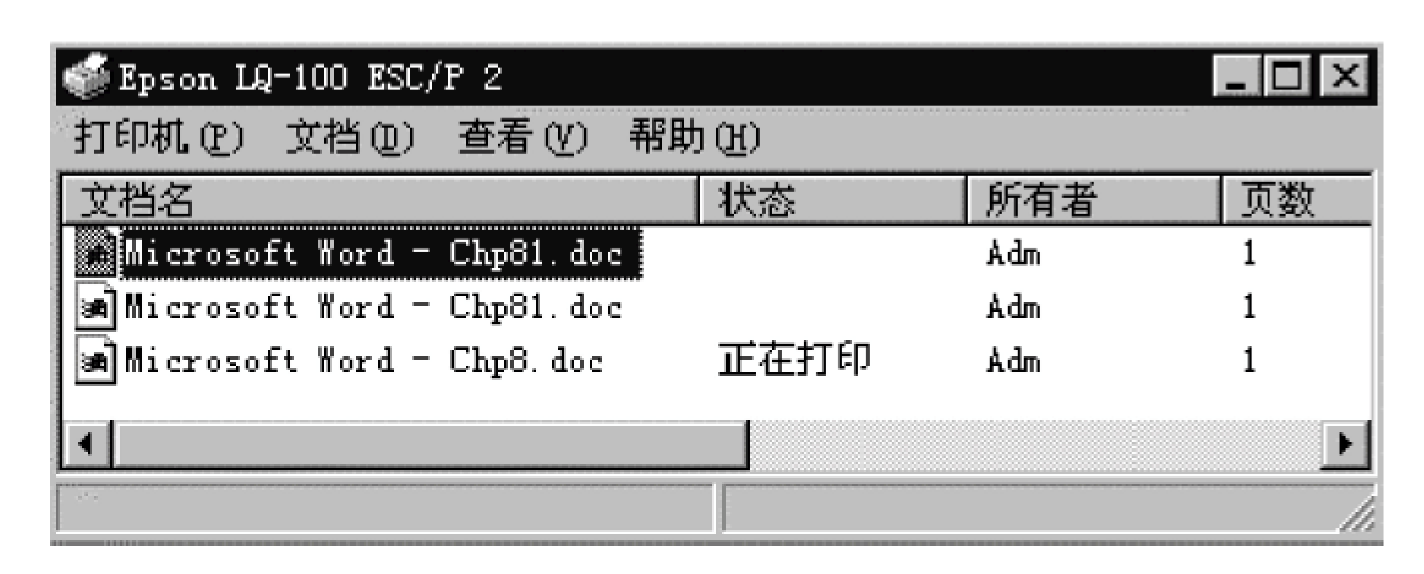


图 11-14 打印管理器窗口中的“打印机(P)”文档

(2) 删除打印文件

① 在图 11-14 所示的打印管理器窗口中，选中拟删除的打印文件名。

② 按键盘的 Del 键，或选择窗口菜单的“打印机”→“清除打印文档”命令选项，均可以删除选中的正在打印的文档。

(3) 暂停打印文件

① 在图 11-14 所示的“打印管理器”窗口中，选中拟暂停的打印文件名。

② 在图 11-14 所示的窗口中，依次选择“打印机(P)”→“暂停打印(A)”命令选项。

说明：

① 打印作业被暂停之后，“暂停打印(A)”命令选项旁边将标记有“√”。需要恢复时，再次选中此项，就可恢复打印。

② 应当注意的是，只能暂停本地打印机的打印工作，而不能暂停网络打印机的打印进程。

(4) 改变打印文件的执行顺序

用户打印的文件输出到网络打印机后，若此时的打印机空闲，则输出的文件可以立即打印。但是，如果用户的打印文件很多，则需要排队等候。如果某用户的文件急于输出，网络管理员可以采用如下步骤进行控制和调整：

① 依次选择“开始”→“设置”→“打印机”命令选项，激活图 11-4 所示的“打印机”窗口，双击需要管理的“打印机”图标，即可打开如图 11-14 所示的“打印管理器”的用户监视窗口。

② 在激活的图 11-14 所示的窗口中，从多个等待打印的文件中，选择需要改变打印顺序的文件后，依次选择“打印机”→“属性”命令选项，激活如图 11-15 所示的窗口。

③ 在图 11-15 所示的窗口中，可以更改选中打印文件 chp8.doc 的优先级。例如，提高打印文件的优先级，即可改变原有的打印顺序。设置之后，单击“确定”按钮，完成操作。

④ 设置后，在图 11-14 所示的窗口中，可以看到当前文件的打印顺序，原来排在队列最后的 chp8.doc 文件将被提前输出。



图 11-15 “打印机(P)”窗口中被选中文件的属性设置窗口

11.7 打印管理中常见问题的处理

1. 打印工作不正常时的检查和处理步骤

① 检查和确认打印电缆和打印端口的连接无误,打印设备在线连接。

② 确认所使用的打印机配置了正确的打印驱动程序,若还不能正常打印,可通过重装打印驱动程序的方法尝试解决。

③ 确认打印服务器的客户机已选中了一个打印机,或者在应用程序中明确指定了所要用的打印机。当然,也可以在打印管理器中设置默认的打印机。

④ 在硬盘上应留有足够的空间来生成打印作业。

⑤ 如果在 Windows NT 中可以正常打印,而在 MS-DOS,OS/2 或 Windows 3.x(Win16)中不能正常打印,应按各工作站上设置和使用“网络打印机”的方法进行检查。

⑥ 某文件打印过程中出现故障,使得其他打印工作不能进行时,应通过打印管理器暂停或删除该打印进程,以使其他打印进程能够正常进行。

2. 常见打印故障问题的处理实例及解决办法

问题 1:来自 DOS 应用程序的打印作业,在 DOS 提示符下,已提交给打印机却打印不出来,应如何解决?

解答:MS-DOS 程序必须在本地安装有适当的打印机驱动器,因此不能完全依赖 Windows NT 来处理它们的打印作业,另有一些 DOS 应用程序,只有在 NT 终止之后才能打印。

问题 2:已将打印作业提交给打印机,打印出来的结果却不正确,应如何解决?

解答:打印机驱动不正确、或不匹配,或者打印处理器损坏了,应重新设置或安装。

问题 3:打印作业在假脱机时阻塞了,不能删除或取消,应如何解决?

解答：停止或启动假脱机服务(spooler service)来清除该作业。

问题4：硬盘开始闪烁，而打印作业并没有发送到打印服务器，应如何解决？

解答：假脱机的硬盘空间用完了，因此必须为假脱机另外指定一个分区。应在registry中进行修改。

问题5：由于应用程序的运行使得打印处理速度过程变慢，应如何解决？

解答：这是由于假脱机的优先级不够高，因此应在registry中\HKEY _local machine\System\CorrentControlSet\control\print\priority class修改优先级的值。

习题

(1) 网络管理员在打印管理中的基本职责有哪些？

(2) 打印服务子系统的建立的主要过程有哪些？什么是打印服务器和打印客户机(工作站)？

(3) 在NT中"打印机"和"打印设备" 分别指什么？为什么将打印机和打印设备分开？

(4) 物理打印端口和逻辑打印端口之间有何区别？

(5) 如何在各种网络工作站上使用网络上的共享打印机？请说明可以安装和设置共享打印机的有效账号有哪几个？如何使不同用户享有不同的打印机使用权限？

(6) 网络"打印机"的连接方式有几种？为一台打印设备创建多个打印机的目的是什么？为一台打印机连接多个打印设备的目的又是什么？

(7) 在什么情况下选择"打印机池"的连接方式？使用此方式的优点有哪些？

(8) 某公司局域网内有3台同型号的惠普激光打印机，请设计并选择这些打印机的连接方式，并说明这种连接方式的组织优点。

(9) 在DOS、Windows 95/98/NT工作站上应当如何使用网络打印机？添加打印机的方法有几种？分别写出服务器和工作站上的主要步骤。

(10) 打印中常见的问题有哪些？各应如何处理？

(11) 如何启动打印管理器？它有那些功能？如何改变打印文件的输出顺序？

实训题目

1. 建立打印服务子系统。

① 建立网络打印服务器。即安装打印设备，配置打印机。

② 配置打印工作站。分别在DOS、Windows 95/98、NT Workstation和NT Server为系统平台的网络打印工作站上，设置、连接和使用网络共享打印机。

2. 在网络打印服务器中进行打印管理。

例如，为不同用户设置不同的打印机使用权限，更改正在打印的用户文档的优先级。



第12章 远程访问服务系统管理

本章将学习与“远程访问服务”有关的基本概念，以及在NT网络中，网络管理员应掌握的实现远程访问服务系统基本功能的必备的操作技能。

主要内容：

- “远程访问服务”(RAS)的作用和基本概念；
- 远程访问服务(RAS)服务器的安装和配置；
- 各种远程访问客户工作站的安装和配置；
- 远程访问服务(RAS)服务器的常规管理。

12.1 远程访问服务的概述

随着计算机网络在各个领域中的推广和应用，越来越多的用户要求在家里或者出差在外时，也能对公司的数据、邮件和其他信息资源进行远程访问，以便对紧急事务进行远程处理。目前，这一切要求都能通过远程访问服务系统来实现。

在NT Server 4.0版中，提供远程访问服务的软件名称为RAS。

12.1.1 远程访问服务的基本概念

1. 远程访问服务—RAS

“远程访问服务”的英文缩写为RAS(remote access service)。远程访问服务就是指在办公室以外的用户通过电话线或其他传输介质远程连入局域网，并存取其中的共享资源，从而使办公地点扩展到办公室以外的任何地方。

2. 远程访问服务系统的建立和管理

远程访问服务系统的建立和管理包括以下3个部分：

(1) RAS服务器

建立远程访问服务系统时，最主要的步骤就是建立RAS服务器。在NT网络中，安装了RAS软件的NT服务器就称为RAS服务器。

(2) RAS工作站

RAS工作站就是远程客户使用的计算机。目前,电话网是世界上应用最为广泛的网络,远程工作站通常使用"调制解调器"(modem)+"电话线",或其他远程连接的方法,通过客户本地机上的"拨号网络"拨入RAS服务器。RAS服务可以使得远程用户从任何一处具有电话网的地方,连接到本地网络上,并对网络资源进行访问或管理。由于RAS支持广域网连接(WAN),因此,一旦远程客户通过RAS服务器登录到本地网络,他的工作就好像在本地进行一样。

(3) 使用RAS服务器管理远程工作站和客户

远程访问系统正是通过RAS服务器对网络上的远程客户和远程工作站上的资源进行控制和管理,同时RAS服务器还提供远程客户的拨号访问服务。

12.1.2 远程访问服务器的设计

综上所述,RAS的主要作用就是提供远程拨号访问服务,如果用户所在的单位拥有连入Internet的专线,就可以为网络内的全体用户提供拨号连入Internet的服务功能。

设计和配置RAS服务器时,应从RAS系统所需的硬件和软件两个方面进行考虑。

1. RAS服务器的软件设计

RAS服务器实际上充当了远程客户和本地网络之间的网关。当RAS服务器作为网关或路由器时,允许使用不同网络传输协议的客户机相互传递信息。

(1) 网络安全性的设定

网络的安全性是网络设计时需要考虑的一个重要因素。如果用户的网络资源很重要,为了防止网络黑客对公司内部网络的破坏,配置用户拨号访问时,可以限制其只能访问RAS服务器本身,而不能访问整个网络。在这种设计中,用户所需要的资源必须都放在RAS服务器上,因此,公司员工使用网络的灵活性和方便性必然会受到影响。

(2) 网络协议的设置

由于网关和路由器都是针对具体的网络通信协议而设定的,因此,配置RAS充当网关或路由器的实质就是配置网络通信协议。如果服务器上安装有多种网络通信协议,则可以在安装RAS服务器时,分别指定每种协议是否充当网关或路由器。

应该注意,RAS服务器对每种协议的支持是不同的。常见的协议有NetBEUI协议、TCP/IP协议和IPX/SPX协议。如果在RAS服务器上将TCP/IP协议和IPX/SPX协议指定为路由服务,则实际上只安装了一个IP路由器和IPX路由器。例如:如果拨号客户机只使用了TCP/IP协议,则远程客户通过RAS服务器就只能访问那些安装了TCP/IP协议的计算机。与之类似的是,对于那些只使用了IPX/SPX协议的客户,通过RAS服务器就只能访问那些安装了IPX/SPX协议的计算机。因此,应该根据实际情况来确定RAS服务器上所配制的协议,以及每种协议是否需要充当网关或路由器。

2. 远程访问服务器的连接硬件

由于RAS服务器需要向客户机提供拨号服务,所以它应当配置有多个调制解调器和多条电话线。调制解调器数量的多少,应根据远程访问客户的数量而定。

如果远程用户数量不多,则可以分别使用几个单独的电话号码的电话线,而无需申请专门的中继线。如果用户比较多,则应考虑申请中继线,这样使用一个电话号码就可以同

时连入多个电话。但是，在这种情况下，还需要购买一块多端口卡，并将其安装在 RAS 服务器上，以便连入更多的调制解调器；当然，用户也可购买专用的远程访问服务器，其连接方法见第 3 章。

3. 远程访问服务器与客户机的通信连接方式

任何微软的 RAS 客户机都可以连入到微软的 RAS 服务器上。一般 RAS 服务器和 RAS 客户机的通信连接方式有以下几种：

① 使用“PSTN”和调制解调器(modem)　RAS 客户机和服务器之间可以使用标准 modem 和 PSTN(公用交换电话网络)进行连接。使用此方法进行连接时要求 RAS 客户机和服务器端都要安装一个 modem，客户机端不需要网卡，因为 modem 已起到了网卡作用。

② 使用“X.25”分组交换网和用户接入设备　X.25 是一种使用包交换协议进行数据传输的广域网，利用这种广域网作为媒介也能实现 RAS 服务器和客户机之间的连接。一个拨号的 X.25 网络客户机能通过 X.25 的用户终端设备和 PAD(分组装配器和拆卸器)接入 X.25 网络，并接入 RAS 服务器。

③ 使用“综合服务数字网”(ISDN)和 ISDN 终端设备　ISDN 是 integrated services digital network 的英文缩写，它的中文名称为“综合服务数字网”，也可称作“综合业务网”。这是一种比 PSTN 具有更快连接速度的数字系统。使用 ISDN 时，要求服务器端和客户工作站端都要安装和使用 ISDN 终端设备和 ISDN 电话外线。

12.1.3　连接 RAS 服务器和 RAS 客户机的远程访问协议

一般可以通过 SLIP(serial line protocol)或 PPP(point to point protocol)来建立与 RAS 服务器的连接。连接 RAS 服务器和 RAS 客户机的协议可以有以下几种，如图 12-1 所示。

1. SLIP(串行线路 Internet 协议)

SLIP 是通过串行线路寻址 TCP/IP 连接的工业标准，可以在低速串行接口中支持 TCP/IP。现在 Windows NT RAS 客户机可以支持 SLIP，这使得 NT 中的 RAS 客户机可以更容易地访问 Internet。但是，SLIP 不支持 IPX/SPX 和 NetBEUI 协议。另外，Windows NT 中的 RAS 服务器中没有支持 SLIP 的组件，因此它不能充当 SLIP 的服务器。

2. PPP(点对点协议)

PPP 是对原来 SLIP 标准的增强。PPP 是一个工业标准协议集，它使远程访问在不同的开发平台上可以进行相互操作。它为点对点的连接提供了标准的发送网络包或数据报的方法。PPP 支持多种协议，其中包括：TCP/IP、NetBEUI、IPX、Apple Talk 等协议。

由上可知，Windows NT 的 PPP 不仅支持 NetBEUI，而且还支持 TCP/IP 和 IPX 连接。用户使用 TCP/IP 协议可以与 Internet 连接；远程用户也可以通过 Windows Sockets 应用程序访问 Internet。由于它支持 IPX，因此，还允许远程用户在 NT Workstation 计算机上通过 CSNW(client service for NetWare，NetWare 客户服务)访问 NetWare Server。

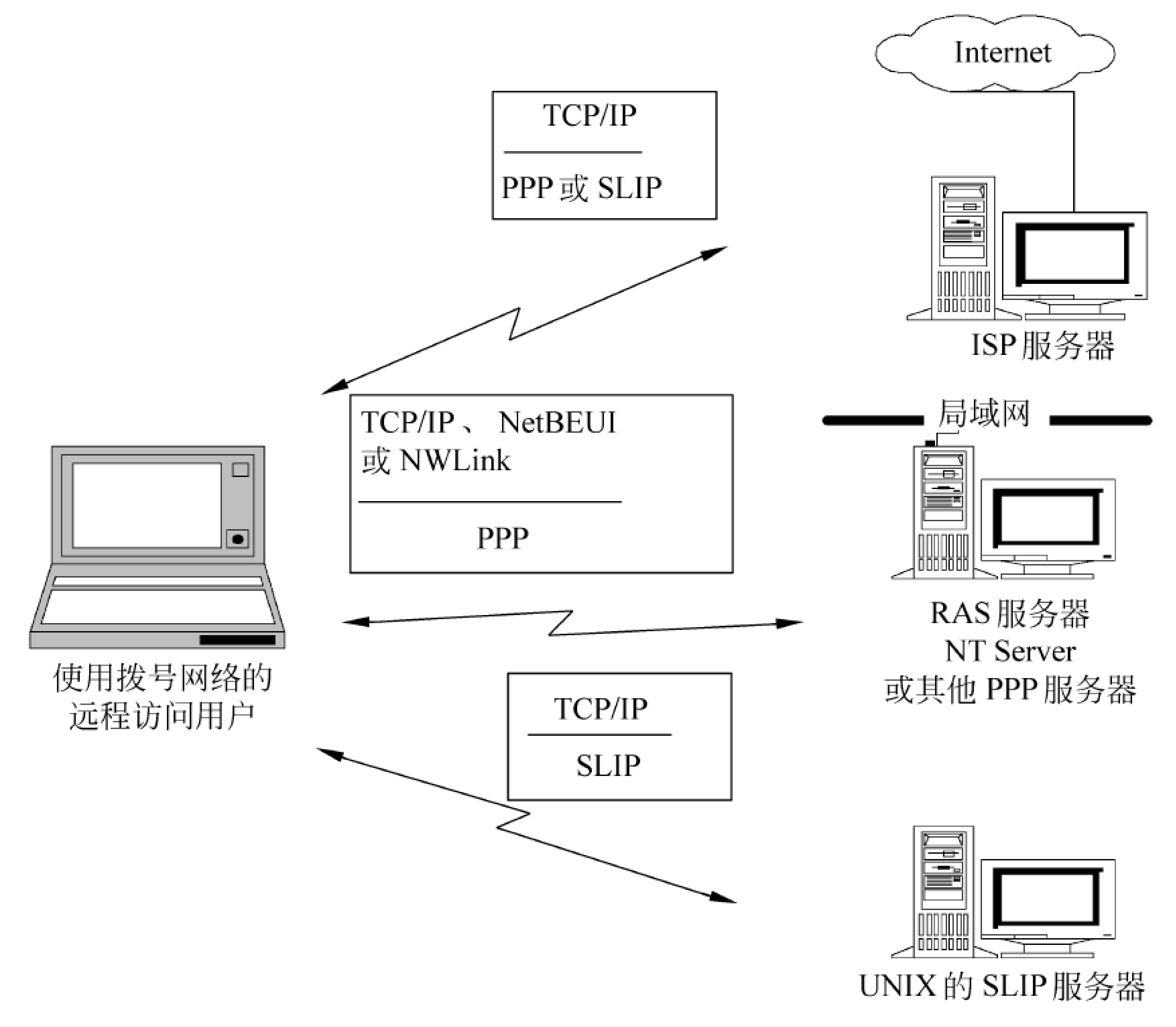


图 12-1 连接 RAS 服务器和 RAS 客户机的协议

3. MP(点对点多重连接协议)

MP 为 multilink ppp 的英文缩写。利用 MP 协议能将多个物理连接合并为一个逻辑连接,这将增加数据传输的带宽。不过它要求客户机端和服务器端都要安装多个 modem、ISND 卡或者相应的 ISDN 终端设备和 X.25 卡等,并且都要配置为允许 MP。

12.1.4 远程访问服务的主要特点

1. **RAS 服务器支持的远程拨入客户工作站和服务器的系统类型**

① 微软客户系统。例如,使用 Windows95/98/NT/2000 平台的 RAS 客户机。

② 非微软客户系统。例如,使用 UNIX 的远程客户机拨入并连接到微软服务器。

2. RAS 支持的网络接口

任何使用下列接口的网络应用程序都可以通过 RAS 运行。

① Windows Sockets　网络计算机间数据输入输出的双向通道。Windows Sockets API(应用程序接口)是一种网络的应用程序接口,程序员可以用来创建 IPX 或 TCP/IP Sockets 的应用程序。

② NetBIOS　网络输入输出系统,用于连接网络资源的软件接口,即用软件实现的输入输出系统。

③ Windows NT 网络 API(WIN32)和 LAN Manager API　网络应用程序的编程接口,用来调用 Windows NT 和 LAN Manager 操作系统的函数。

④ RPC(远程过程调用)　消息传送设备,它允许一个分布式应用程序调用网络上不

同计算机的可用服务，在远程管理时很有用。

⑤ 邮件槽(mailslots)　一个消息发送系统。

⑥ 命名管道(named pipe)　进程通信机制，允许一个本地或远程的进程通信。

3. Windows NT RAS 连接的限制

① Windows NT Server　在服务器中 RAS 支持多达 256 个同时连接的远程工作站。

② Windows NT Workstation　在 NT 工作站中 RAS 只支持 1 个远程工作站的连接。

③ 多串口设备　例如，Digiboard 适配器可以为 RAS 服务器提供多个串口。Digiboard 适配器的驱动器随 Windows NT Workstation 和 Server 软件一起发售。

④ RAS 压缩软件　使用 RAS 软件压缩时比不使用时的连接速度可以高出多倍。

⑤ 多处理器　RAS 服务器是多线程的，可以扩充为多个 CPU。在多 CPU 的计算机上，RAS 服务器的线程可以同时在多个处理器上运行。因此，使用多处理器可以极大地提高 RAS 的性能。

4. Windows NT RAS 连接的安全性

Windows NT RAS 制定了以下一些安全性措施，以确保只有合法的远程用户才能访问网络上的资源：

① 集成域的安全性　RAS 服务器采用与 Windows NT 计算机完全相同的账户数据库。因此，若要连到 RAS 服务器上，用户除了有一个合法的 Windows NT 账户外，还必须具有 RAS 的拨入(dial-in)许可，在试图登录到 Windows NT 之前必须得到 RAS 的验证。

② 加密验证和登录　所有验证和登录信息(如用户名，口令)在电话线路上传输时都可以被加密。

③ 审核　RAS 可以为所有的远程连接产生审计信息，包括验证和登录等活动。

④ 第三方主机(中介安全性)　通过在 RAS 客户机和服务器之间连接一个第三方中介安全性主机，可以为 RAS 设置另一级安全性。当使用第三方中介安全性主机时，在与 RAS 服务器建立一个连接之前，用户必须要输入口令或代号才能够通过安全性设备。

⑤ 回呼安全性　为了增加安全性，可配置 RAS 服务器，以提供回叫。即通过 RAS 服务器拨叫远程用户来验证与本地网络的连接，可以增加另一级安全性。

⑥ PPTP 过滤器　使用 PPTP 技术时，RAS 服务器可直接与 Internet 和公司内部的局域网相连，因此有可能给公司内部造成不安全因素。当使用 PPTP 过滤器功能后，所有非 PPTP 的协议在网卡上都将被禁止，从而提高了安全性。

12.2　远程访问服务器的安装与配置

在建立远程访问服务系统时，最主要的工作就是安装和配置 RAS 服务器。

12.2.1　RAS 服务器安装之前的准备工作

安装 Windows NT“RAS”之前应做好如下准备工作：

① RAS 服务器所使用的通信端口号。

② RAS 服务器使用的调制解调器(modem)。

③ 在 RAS 服务器的“控制面板”中,安装、设置好 modem。

④ 确认网络的访问方式。例如:是拨入本台计算机,还是访问整个计算机网络;是只“拨出”,还是“既拨入又拨出”等。

⑤ 应成功加载系统硬件所需的各种硬件驱动程序。

12.2.2 安装 NT 中的 RAS 服务器

安装 NT“RAS”服务器的步骤如下:

① 依次选择“开始”→“设置(S)”→“控制面板(C)”命令选项,在打开的“控制面板”窗口中,选择“网络”图标。

② 在激活的“网络”窗口中,选择“服务”选项卡。

③ 在“服务”选项卡中,单击“添加(A)”按钮,激活如图 12-2 所示的窗口。

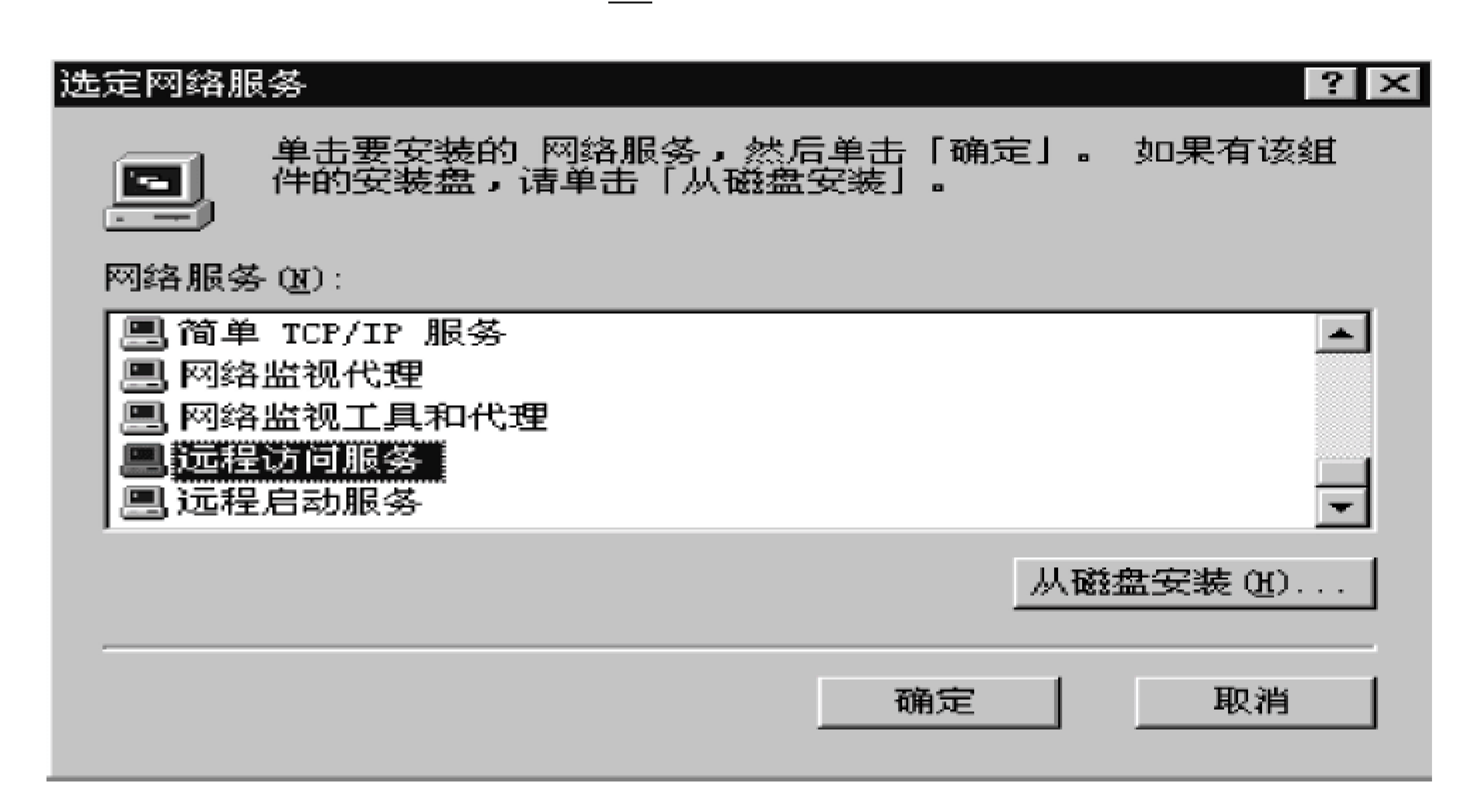


图 12-2 “选定网络服务”窗口

④ 在图 12-2 所示的窗口中,选择“远程访问服务”选项后,单击“确定”按钮。

⑤ 根据提示插入 NT Server 的 CD-ROM 盘,然后单击“继续”按钮。

⑥ 当系统中出现或检测到新的“RAS”设备时,激活如图 12-3 所示的窗口。



图 12-3 “添加 RAS 设备”窗口

⑦ 图 12-3 所示的窗口提供了添加“检测到的 RAS 设备”、“调制解调器”、“安装新设备或其他的 RAS 可用设备(PAD)”的机会。例如,单击“安装调制解调器(M)”按钮,将激活调制解调器的安装窗口,从中选择“不检测调制解调器”选项后,可以使用调制解调器自

带的驱动程序安装和设置。最后,单击“确定”按钮,激活如图 12-4 所示的窗口。



图 12-4 “安装远程访问”窗口

⑧ 在图 12-4 所示的窗口中,可以删除、添加或配置远程访问的可用端口。例如,单击“配置”按钮,激活如图 12-5 所示的窗口。

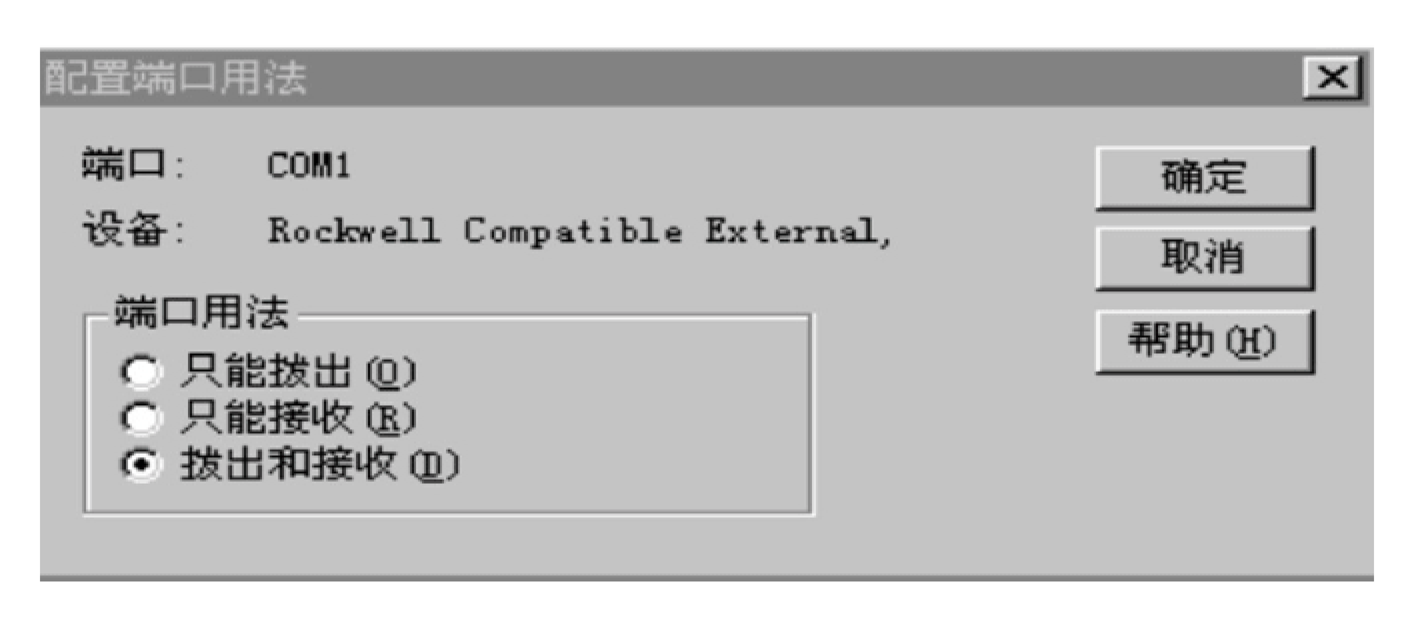


图 12-5 “配置端口用法”窗口

⑨ 在图 12-5 所示窗口中的“端口用法”栏目下,选择“拨出和接收”单选钮,然后单击“确定”按钮,返回图 12-4 窗口。有关图 12-5 的设置说明如下:

- 只能拨出(O) 表示这台计算机只能充当 RAS 客户机。
- 只能接收(R) 表示这台计算机只能充当 RAS 服务器。
- 拨出和接收(D) 表示这台计算机既可充当 RAS 客户机,也可以充当 RAS 服务器,但同一时间内只能扮演一个角色。

⑩ 在图 12-4 所示的窗口中,选择“网络(N)”按钮,激活如图 12-6 所示的窗口。

⑪ 在图 12-6 所示的窗口中,可以设置拨出和拨入的协议,加密的设定等多项内容。例如:选择“拨出和接收”单选钮后,单击“确定”按钮,返回图 12-4 窗口。在图中选择“网络(N)”按钮,再次激活如图 12-6 窗口,可以继续进行设置。有关图 12-6 的设置说明如下。

- 拨出协议 设置这台计算机拨出时所使用的协议。
- 服务器设置 设置此计算机充当 RAS 服务器时,允许工作站拨入并设置工作站所使用的通信协议。
- 由于 Windows NT 和 Windows 95/98 工作站拨入时,可以使用 NetBEUI、NWLink(IPX)与 TCP/IP 协议,而 DOS、LAN Manger、Windows 3.1 和 Windows for workgroup 等工作站的 RAS 只支持 NetBEUI。因此,RAS 服务器

上应当安装和配置所有远程工作站需要使用的协议。



图 12-6 “网络配置”窗口

⑫ 在图 12-6 所示的窗口中，选中 NetBEUI(B)选项后，单击“配置”按钮，在图中，可以对 NetBEUI 协议进行配置，NetBEUI 协议是 RAS 服务器上 3 种协议中最容易配置的，因为它不需要任何额外的参数。选中“整个网络”单选钮，单击“确定”按钮，返回图 12-6 所示的窗口。

⑬ 在图 12-6 中选择 TCP/IP(P)复选框后，单击“配置”按钮，激活如图 12-7 所示的窗口，选择之后，单击“确定”按钮，返回如图 12-6 所示的窗口。

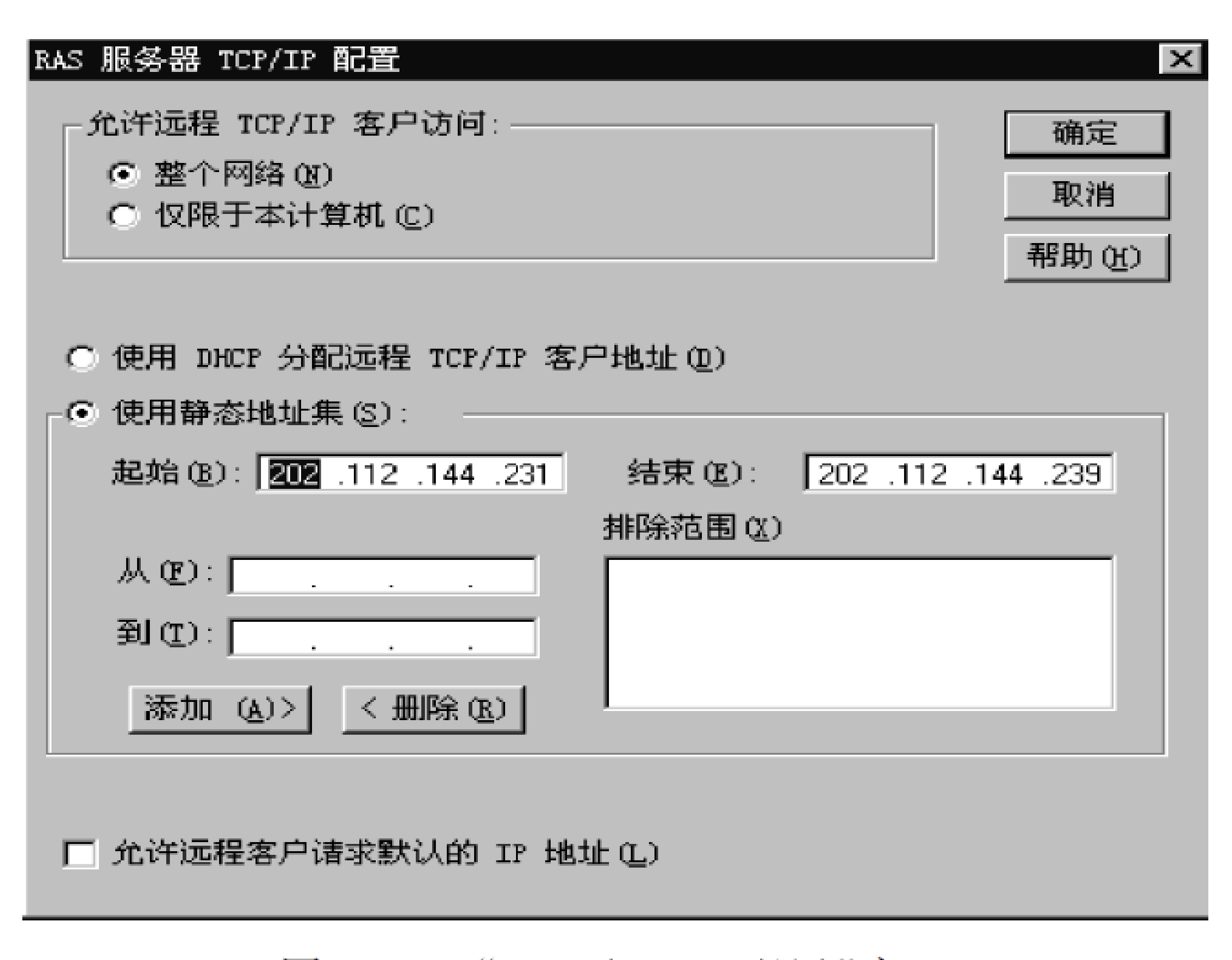


图 12-7 “TCP/IP(P)配置”窗口

有关图 12-7 的设置说明如下：

- 整个网络(N)　若选择此项，则允许 RAS 服务器充当 IP 路由器，从而允许使用 TCP/IP 协议的远程用户访问整个网络。

- 仅限于本计算机(C)　远程用户只能访问 RAS 服务器上的资源。
- IP 地址的设置　因为使用 TCP/IP 协议的 RAS 客户机需要一个 IP 地址，因此必须设置可用的 IP 地址。

设置 IP 地址的方法和注意事项如下所述：

- 使用 DHCP 服务器分配 TCP/IP 客户机地址　若 RAS 客户机没有配置静态 IP 地址，则当远程客户连入 RAS 服务器时，DHCP 服务器将为它自动分配一个 IP 地址。
- 使用静态地址集　如果网络上没有 DHCP 服务器，可以在 RAS 服务器上设置一个 IP 地址的范围（“起始”～“结束”），此范围必须对本地子网有效，且不能被 RAS 服务器所属的子网使用。当 RAS 工作站拨号连入 RAS 服务器时，RAS 服务器就从这段地址中挑选一个 IP 地址给它。注意，如果网络上使用了 DHCP 服务器，而又没有为 RAS 客户机分配 IP 地址，那么这段地址的范围必须被排除在 DHCP 服务器地址范围之外。
- 允许远程客户请求默认的 IP 地址若 RAS 客户已经预先配置了一个 IP 地址，则应选中此选项。

⑭ 在图 12-6 所示的窗口中，选中 IPX(X)复选项之后，单击旁边的“配置”按钮。在激活的图中可以对其进行配置，配置之后，单击“确定”按钮，仍返回图 12-6 所示的窗口。

各项配置结束后，单击“确定”按钮，RAS 服务器上的设置结束，重新启动计算机后设置生效。

12.3　远程访问客户工作站的安装与配置

在远程访问服务系统中，另一项重要工作就是为客户使用的各种远程工作站做好远程登录的准备。

12.3.1　远程访问服务客户工作站上调制解调器的安装

使用 NT 的 RAS 客户工作站包含两种，一种是 NT Server(即非 RAS 服务器)；另一种是 NT Workstation。在这两种工作站上安装调制解调器的过程十分相似，其主要步骤如下：

① 依次选择“开始”→“设置(S)”→“控制面板(C)”命令选项，在打开的“控制面板”窗口中，选择“调制解调器”图标，激活如图 12-8 所示的窗口。

② 在图 12-8 所示的窗口中，单击“添加”按钮。如果安装的是列表中未列出的 modem，则在打开的窗口中，选择“不检测调制解调器...”→“从磁盘安装”命令进行安装。

③ 之后，在图 12-8 所示的窗口中，选中所安装的 modem，单击“属性”按钮。在激活的窗口中，可设置或调整 modem 的参数。例如调整速率，选择最快的速率为 115 200，或者调整扬声器的音量大小等。



图 12-8　RAS 客户端“调制解调器 属性”窗口

12.3.2　远程访问服务工作站上拨号网络的安装和配置

远程访问服务工作站上拨号网络的安装和配置步骤如下：

① 依次选择“开始”→“程序(P)”→“附件”→“拨号网络”命令选项，首次启动时，会启动安装向导，跟随屏幕提示，即可完成所有安装过程。如果非首次安装，将激活如图 12-9 所示的窗口。



图 12-9　RAS 中拨号网络—“新的电话簿项向导”窗口

② 在图 12-9 所示的窗口中，先设置要呼叫的 RAS 服务器的名称，例如 MyDialUpServer；然后，单击“下一步(N)”按钮，激活如图 12-10 所示的窗口。

③ 在图 12-10 所示的窗口中，可以选择要呼叫的远程服务器，如果是连入 Internet，可选中第一选项；如果是连入 NT 网络的 RAS 服务器，可选中第二选项。选择之后，单击“下一步(N)”，激活后继的窗口。

④ 在激活的“电话号码”窗口中，输入要呼叫的远程服务器的电话号码。

- 如果是连入 Internet，此处应输入用户 ISP 的电话号码。
- 如果是连入 NT 网络的 RAS 服务器，此处应输入 RAS 服务器的电话号码。



图 12-10　RAS 中拨号网络的配置—“服务器”窗口

⑤ 当 RAS 服务器有多个可拨叫的电话号码时，还可以输入其他“候选”号码。这样，当首选电话号码连接不通时，系统会自动使用候选的电话号码。选择之后，单击“下一步(N)”按钮，在激活的窗口中，单击“完成”按钮，激活如图 12-11 所示的窗口。



图 12-11　“拨号网络”呼叫窗口

⑥ 在图 12-11 所示的窗口中，从“用于拨号的电话簿项(R)”下部窗口中，选择拟呼叫的远程服务器；也可以单击“其他”按钮，修改有关设置；若单击“拨号”按钮，激活如图 12-12 所示的窗口。



图 12-12　连接到“RAS”服务器的窗口

⑦ 在图 12-12 窗口所示中，输入在拟登录服务器上有效的“用户名”、“密码”和“域”名后，单击“确定”按钮。开始拨号，并进行用户名和密码的验证。

⑧ 成功登录后，在窗口右下角，将出现“拨号网络监视器”图标，选择此图标，可以激活“拨号网络监视器”—“状态”窗口，在该窗口中，显示了各种状态信息。例如线路连接速度、连接持续时间等。选择其中的“摘要”选项卡，激活后继的窗口。

⑨ 在激活的“拨号网络监视器”—“摘要”选项卡窗口中，若单击“挂断”按钮，则断开此次连接。若单击“详细资料”按钮，则激活如图 12-13 所示的窗口。



图 12-13 “详细资料”选项卡窗口

⑩ 在图 12-13 所示的窗口中，用户可以了解到此次网络注册的详细信息。例如使用的 IP 地址等。

12.4 远程访问服务器的管理

作为系统管理员应该熟练掌握 RAS 服务器的管理界面中各种工具的使用，例如管理 RAS 工作站、查看、管理通信端口和远程客户等。此外，在客户访问 RAS 服务器之前，系统管理员必须使用 RAS 服务器对远程访问系统进行管理，以实现对 RAS 工作站的访问权限的控制和管理。

12.4.1 RAS 服务器管理员的职责

RAS 服务器管理员应当完成的工作如下：

① 为远程访问客户授予访问权限。

② 查看当前的活动连接情况，连接端口的现状，以及连接的性能。

③ 断开连接。

④ 给连接的远程客户发送信息。

⑤ 启动、停止、暂停和继续 RAS(远程访问)。

12.4.2 RAS 服务器的管理

RAS 服务器上的“远程访问系统管理器”是远程访问系统管理的主要工具。

1. 使用“远程访问系统管理器”之前的准备工作

使用“远程访问系统管理器”之前，网络管理员必须做好以下准备工作：

① 管理“远程访问系统管理器”时，首先必须选定管理对象。例如选择服务器或者“域”进行管理，实例中选择了“ZDH-JSJ”主域。

② 网络管理员必须具有选定域的系统管理员的特权。如果选定服务器，则应具有该服务器管理操作员和账号操作员的特权。有了上述权限之后，网络管理员才能管理选定的域或服务器。例如实例中，以“ZDH-JSJ”域中的 administrator 身份登录。

③ 登录之后，网络管理员应当为远程访问客户设置 RAS 拨入许可的权限，这样该远程访问客户才能实际地连入 RAS 服务器。

2. “远程访问系统管理器”的启动

依次选择“开始”→“程序(P)”→“管理工具(公用)”→“远程访问系统管理器”命令选项，激活如图 12-14 所示的窗口。



图 12-14 “远程访问系统管理器”—“服务器(S)”下拉菜单窗口

3. 利用“远程访问系统管理器”选择被管理的对象

在“远程访问系统管理器”中，可以选择被管理的对象。例如，选择域或服务器。

① 在图 12-14 所示的窗口中，依次选择“服务器(S)”→“选择域或服务器”命令选项，激活后继的窗口。

② 在激活的“启动远程访问服务”窗口中的“服务器”文本框中，应输入“域名”或“服务器名”。如果输入的是服务器名，则必须以双反斜杠（\\）开头，例如，\\ NT Server。当然，也可以在“选定域”列表框中选定“域”或“服务器”。选择时，需注意列表框中显示的域是用户机所属域的所有委托域(信任域)。若想查看某个域的服务器，请直接双击选中域的域名。例如，双击“NT Server”(服务器名)。

③ 在网络上浏览时，尤其是在远程工作站进行访问连接的浏览时，访问速度将明显降低。因此，可以关闭指定域的浏览功能。在图 12-14 所示的窗口中，选择“选项(O)”→“慢速连接”命令选项，可以关闭浏览功能。

4. 为远程访问客户授予拨入 RAS 的权限

为远程访问客户授予拨入 RAS 的权限的步骤如下所述：

① 在图 12-14 所示的窗口中，依次选择“用户(U)”→“权限(P)”命令选项，激活如图 12-15 所示的窗口。

② 在图 12-15 所示的窗口中，选择允许拨入的远程访问客户，例如 SXH，然后单击“确定”按钮，完成设置。对图 12-15 所示窗口的设置做如下说明：

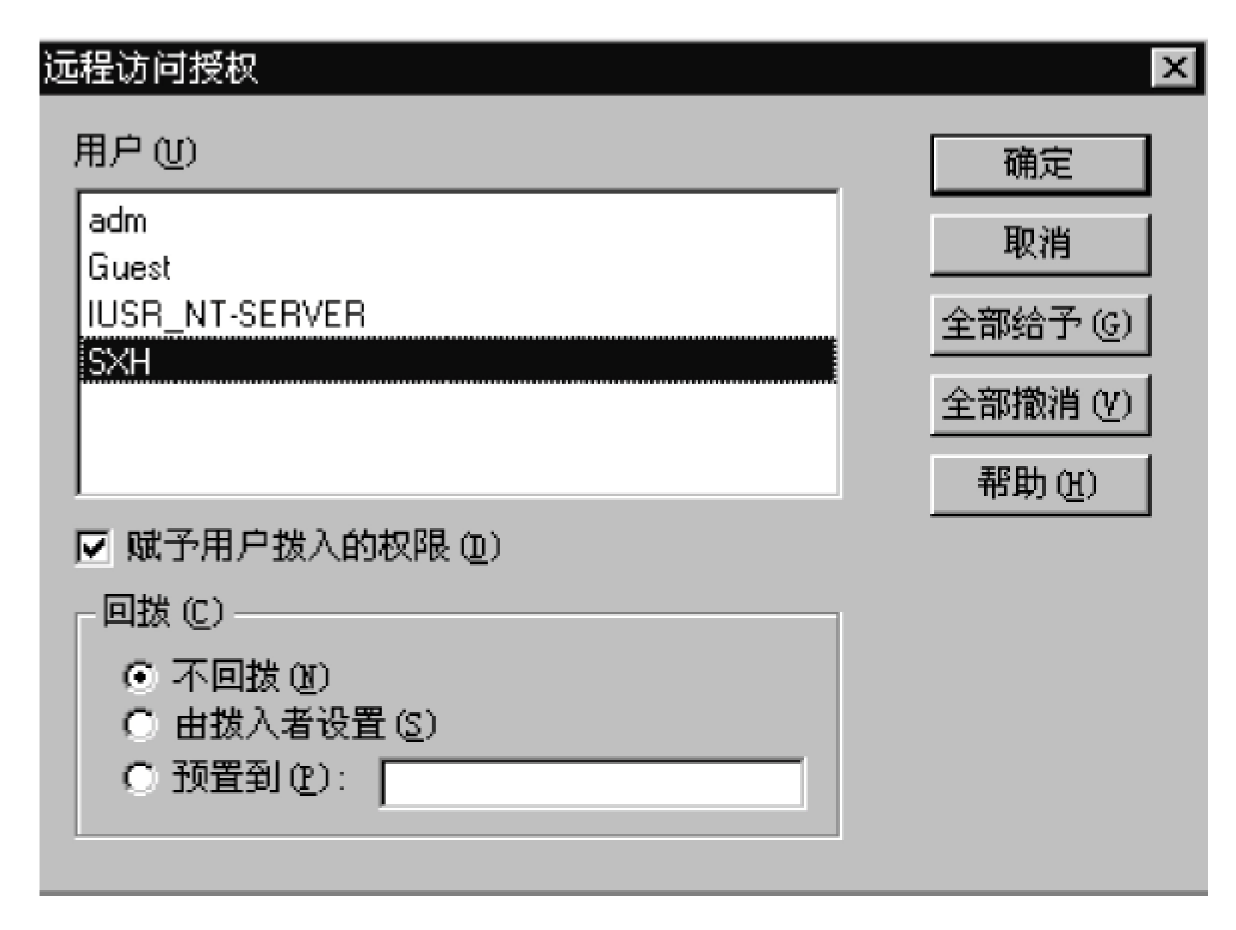


图 12-15 “远程访问授权”窗口

- 不回拨(N) 若选中了此项,则当远程用户拨号进来之后,主要账号和口令都正确时,即可以访问网络。
- 由拨入者设置(S) 由 RAS 工作站决定是否需要回拨。当 RAS 服务器所在地的电话费用比 RAS 工作站所在地便宜许多时,利用此种方式连接可以节约电话费。注意,若选中此项后,即由 RAS 服务器方付费。
- 若同时允许所有的 RAS 客户拨入 可以单击“全部给予(G)”按钮。反之,可以单击“全部删除(V)”按钮,将一次性撤消所赋予的所有远程客户的访问权限。

5. 查看活动中的远程访问客户

① 在图 12-14 所示的窗口中,依次选择“用户(U)”→“活动用户(A)”命令选项,激活如图 12-16 所示的窗口。



图 12-16 活动中的“远程访问客户”窗口

② 在图 12-16 所示的窗口中,显示了正在连接的远程访问客户,例如图中显示了账号为 adm 的用户登录服务器的情况。

③ 在图 12-16 所示的窗口中,单击“用户账号(U)”按钮,在激活的窗口中,将显示活动中的“用户账号”情况。

6. 给活动中的远程访问客户发送信息

给活动中的远程访问客户发送信息的步骤如下:

① 在图 12-16 所示的窗口中,单击“发送消息(M)”按钮,激活后继的窗口。

② 在激活的“发送消息”窗口中,可以给指定的活动的远程用户发送消息,将消息写

入至“消息(M)”文本框中,单击“确定”按钮。远程客户端即可收到所发送的消息。

7. 远程访问服务器的常规管理

使用远程访问服务器进行常规管理有如下项目:

(1) 查看活动中的远程访问客户端口

① 依次选择“开始”→“程序(P)”→“管理工具(公用)”→“远程访问系统管理器”命令选项,激活如图 12-14 所示的窗口。

② 在图 12-14 所示的窗口中,选择“服务器(S)”→“通讯端口(C)”命令选项。

③ 在激活的“通讯端口”窗口中,单击“端口状态(S)”按钮,激活如图 12-17 所示的窗口。在该窗口中,可以进一步查看和了解通讯端口的情况。

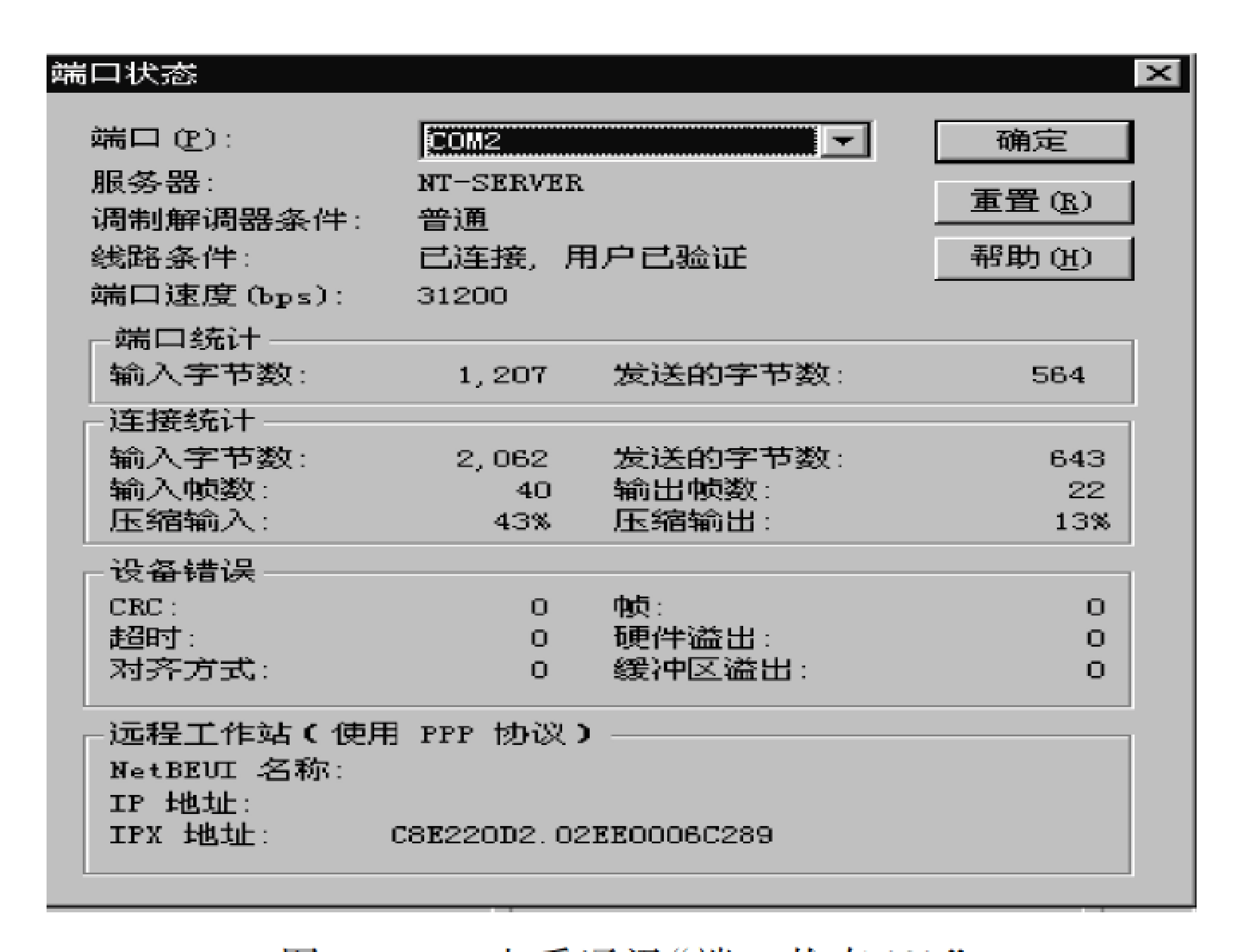


图 12-17 查看通讯“端口状态(S)”

(2) 管理活动中的远程访问服务

① 在图 12-14 所示的窗口中,选择“服务器(S)”,激活其下拉菜单,管理员可以根据需要选择有关远程访问服务的管理。例如:选择“停止远程访问服务(T)”命令选项,激活如图 12-18 所示的窗口。



图 12-18 “停止远程访问服务(T)”窗口

② 在图 12-14 所示的窗口中,管理员还可根据需要选择“服务器(S)”→“暂停远程访问服务(P)”或者“服务器(S)”→“继续远程访问服务(N)”命令选项,可以激活相应的“服

务控制”提示信息窗口。

12.5 各种远程访问工作站端的设置与操作

建立远程访问服务器的目的就是方便客户能够在家中、旅途或任何办公室之外的环境中，使用电话通信线路和调制解调器远程访问局域网上的各种资源。由于客户机的硬件和软件各不相同，因此，远程访问客户端的设置也有所不同，下面分别进行介绍。

12.5.1 从 NT Workstation 客户工作站连入 RAS 服务器

通过 NT Workstation 客户工作站访问 RAS 服务器的步骤如下所述：

① 确认 NT Workstation 工作站上已安装调制解调器（参照 12.3.1 小节）。

② 确认 NT Workstation 工作站中已经安装了“拨号网络”（参照 12.3.2 小节）。

③ 确认 RAS 服务器上已为该远程工作站设置好访问权限（参照 12.4.2 小节）。

④ 使用拨号网络呼叫 RAS 服务器（参照 12.3 节）。

⑤ 使用 RAS 服务器上的各种已共享，并允许访问的软硬件资源。

12.5.2 从 Windows 95/98 客户工作站连入 RAS 服务器

1. Windows 95/98 **客户机工作站连入** RAS **服务器之前的准备**

① 确认 Windows 95/98 工作站上已安装调制解调器。

② 确认 Windows 95/98 工作站中已经安装了“拨号网络”。若没有安装，按以下各步依次进行。

2. Windows 95/98 客户工作站连入 RAS 服务器的设置

通过 Windows 95/98 客户机工作站访问 RAS 服务器的设置步骤如下：

① 依次选择“开始”→“程序(P)”→“附件”→“拨号网络”命令选项，打开“拨号网络”窗口，选择“新建连接”图标，激活后继的窗口。

② 在激活的“创建新连接”窗口中，选择和配置需要使用的调制解调器，并确认或输入拟呼叫的服务器名称，例如“RAS 服务器”。

③ 配置和选择之后，单击“下一步＞”按钮，激活后继的窗口。

④ 在激活的“创建新连接”窗口中，输入所呼叫的 RAS 服务器的电话号码、区号和国家代码等，例如，输入“84021170”后，单击“下一步＞”按钮。

⑤ 在后继的窗口中，单击“完成”按钮，完成“拨号网络”的创建过程。

3. 在 Windows 95/98 客户机上拨叫 RAS 服务器

在 Windows 95/98 客户机上，使用拨号网络呼叫已建立的 RAS 服务器。

① 依次选择“开始”→“程序(P)”→“附件”→“拨号网络”命令选项，打开“拨号网络”窗口，选择建立好的“RAS 服务器”图标。

② 在“连接到”窗口中，输入在 RAS 服务器中具有远程访问权限的用户账号名称和口令之后，单击“连接”按钮，开始“拨号”过程。

③ 稍候，会出现登录、连接和验证等窗口，注册成功之后，在屏幕右下角会出现“已连接到…”窗口。

注意：

- 在 Windows 98 环境下，拨号网络的设置与 Windows 95 大同小异，只有少量的差别，用户可以参照执行。例如，在 Windows 98 中将不出现“后拨号终端屏幕”窗口，系统验证成功后可以直接登录到 RAS 服务器。
- 在“已连接…”窗口中，如果有“详细资料”按钮，单击该按钮可以进一步展开该图，从中可以了解到各种连接信息。

④ 在“已连接到 RAS 服务器”窗口中，单击“断开”按钮，可以断开与 RAS 服务器的连接。

⑤ 使用 RAS 服务器上的各种软硬件资源。连接成功之后，可以使用 RAS 服务器上的各种软件、硬件资源。例如，先在“RAS 服务器”端，设置 CD-ROM 的共享名为“NT-S-F”，然后，就可以在“网上邻居”中单击并使用该共享资源。

12.5.3 从 NT Server 客户机(非 RAS 服务器)连入 RAS 服务器

通过 Windows NT 远程服务器(NT 服务器)访问 RAS 服务器的步骤与 12.5.1 小节介绍的 NT Workstation 工作站类似，其主要步骤简述如下：

① 确认 Windows NT 远程服务器上已安装调制解调器(参照 12.3.1 小节)。

② 确认 Windows NT 远程服务器中已经安装了“拨号网络”(参照 12.3.2 小节)。

③ 确认 RAS 服务器上已为该远程服务器设置好访问权限(参照 12.4.2 小节)。

④ 使用拨号网络呼叫 RAS 服务器(参照 12.3 节)。

⑤ 使用 RAS 服务器上的各种软件硬件资源。

习题

(1) 什么是“远程访问”？它的中文、英文名称各是什么？

(2) 远程访问服务的作用有哪些？

(3) 远程访问管理包括哪 3 个主要部分？

(4) 连接 RAS 服务器和 RAS 客户机的方式有哪些？

(5) 如何安装和配置 RAS 服务器？

(6) 如何为远程访问客户设置可用的 IP 地址？有几种方式？

(7) RAS 服务器所连接的软件和硬件有哪些？

(8) 连接 RAS 服务器和 RAS 客户机的远程访问协议有哪些？各有什么特点？

(9) 根据本章的内容写出网络管理员在远程访问系统中的主要工作职责。其中，RAS 服务器管理员的具体职责又有那些？

(10) 从 NT Workstation 工作站连入 RAS 服务器的主要步骤有哪些？

(11) 从 Windows 95/98 工作站连入 RAS 服务器的主要步骤有哪些？

(12) 如何管理 RAS 服务器上连入的远程活动客户？

(13) 如何在 NT Workstation 工作站上远程访问用户 FTP 资源？客户端的主要设置有哪些？

(14) 如何在各种远程网络工作站上访问 FTP 服务器？服务器端和客户端的主要设置有哪些？

实训题目

1. 在 NT Server 中安装、设置和管理 RAS 服务器。

2. 在 NT Workstation 远程访问客户工作站上设置 RAS 服务器并登录 RAS 服务器。

3. 在 Windows 95/98 和 NT 工作站上远程访问 RAS 服务器中开放的共享资源(目录和文件资源、FTP 和 WWW 信息资源、收取局域网的邮件等)。

4. RAS 服务器的管理工具及其使用，包括：管理账户、发送信息和管理远程工作站等。



第13章 电子邮件系统管理

本章介绍 Intranet 网络中电子邮件系统和电子邮件的基本知识，以及最简单的邮件服务器（工作组邮局）及其客户工作站的安装、使用和配置等内容。

相信读者在深刻理解本章的内容之后，便可以轻松地建立、使用和管理更为复杂的电子邮件系统了。

主要内容：

- 网络邮局和电子邮件（E-mail）的基本知识；
- 邮件服务器（工作组邮局）的建立和管理；
- 在各种邮局工作站上收发局域网的电子邮件；
- 使用网络邮局收发文本、图形或其他类型的邮件；
- 在 Windows 98 上启用网络工作组邮局。

13.1 电子邮件服务系统

E-mail 是网络中使用最频繁的一种服务，也是一种与其他用户进行联系的快速、高效、简便和廉价的通信形式，可以将电子邮件服务系统形象地称为“网络邮局”，它是信息高速公路中 E-mail 传递的中转站，人们通过它，在网络上传递公文和各种不同形式的文件。无论在办公室，还是出差在外，当需要收发 E-mail 时，只要通过传输介质，就能访问在“网络邮局”内的 E-mail。因此，电子邮件系统的创建、管理和使用是每一个网络管理员必不可少的一项基本技能，也是网络管理员在邮件管理中的工作目标和基本职责。

1. 电子邮件服务系统的功能

E-mail 的中文名称为电子邮件。Intranet 中 E-mail 的服务是当今网络中不可缺少的也是使用最多的一项基本服务，因此，E-mail 系统是 Internet 和 Intranet 上的主要功能系统之一，其主要作用是让网络中的客户能够通过网络电子邮件服务系统有效而快速地交换各种信息。

(1) E-mail 系统的工作模式

E-mail 系统同样采用了客户/服务器模式。网络管理员通常先在 E-mail 服务器的磁

盘中，为用户建立起存放和交流电子邮件的专用存储空间，并由 E-mail 服务器进行统一的管理，而用户则使用安装在客户工作站上的 E-mail 客户端软件，通过网络邮局收发电子邮件。

（2）E-mail 系统的功能

① 邮件的编辑　包括电子邮件的起草、修改和编辑。

② 邮件的发送　电子邮件系统可以将电子邮件发送给一个或多个用户。

③ 收件的通知　电子邮件系统可以提示用户读取收件箱中的邮件。

④ 邮件的读取　电子邮件系统可以检索、提取和阅读电子邮件。

⑤ 邮件的回复与转发　电子邮件系统可以按电子邮件的地址回复与转发邮件。

⑥ 邮件的退回　当发送邮件的地址有误时，电子邮件系统应当能够将该邮件退回给发送者，并说明原因。

⑦ 邮件的管理　电子邮件系统能够对电子邮件进行管理。

⑧ 邮件的安全保密　通过设置用户名和密码等实现电子邮件的安全和保密。

2. 电子邮件服务系统的组成

电子邮件服务系统主要由 3 部分组成。其一，硬件由服务器和客户机组成；其二，软件分别由电子邮件服务器端软件和客户端邮件软件组成。其三，通信协议。

（1）电子邮件服务器端软件及协议

电子邮件服务器的作用主要是向用户提供电子邮件信箱，负责安全地收、发和管理电子邮件。电子邮件服务器通常使用 SMTP（simple mail transport protocol，即简单邮件传送协议）来传送 E-mail。SMTP 描述了文本形式的电子邮件传送格式和方式。对于二进制数据和文件，则使用 MIME 协议（即多用 Internet 邮件扩展协议）。

服务器端可以使用的、能够支持电子邮件系统的软件有许多种，常用的有 Microsoft Exchange Server、Lotus Notes、Novell Group Wise 和 Windows 95/NT 中内置的工作组邮局等软件。

当网络中安装了高级电子邮件系统，例如：安装了 Exchange Server 时，则可以利用它建立起局域网的电子邮件服务器；而对于要求不高的小型网络来说，则可以利用 Microsoft Mail 建立电子邮件系统，这就是本章所要介绍的 Microsoft Mail 工作组邮局。

（2）电子邮件工作站端软件

电子邮件客户机上常用的电子邮件软件有 Fox Mail、IE5.0、Netscape 4.06、Office 中的 Outlook 和 Windows 98/Me 中的 Outlook Express 等，支持工作组邮局工作站的有 Windows 95/NT/2000 中内置的客户机邮件软件 Microsoft Exchange 等。

13.2　网络电子邮件系统的建立

在 NT 网络中，电子邮件服务子系统的建立就是指网络工作组邮局的建立，它分为提供邮件服务的邮件服务器（邮局）端和使用邮件服务的邮件客户端两个方面。

13.2.1　网络电子邮件系统的职能

网络电子邮件系统就是指网络邮局系统。在使用“网络邮局”之前，应当知道什么是“网络邮局”，以及它应具有的主要职能。

① 从职能来看，“网络邮局”的职能与邮政局类似，它是网络中的电子邮件和信息传递的中转站。正像邮件需要通过邮政局传递一样，网络中的各类电子邮件必须通过“网络邮局”才能传递到用户的计算机的“收件箱”中。

② 电子邮件系统包含一组管理网络邮局用户的工具软件，可以用来添加、删除或修改用户的有关信息。

③ 电子邮件系统包含的一个通信软件正是用户彼此联系的窗口，这就是我们所说的“Windows Messaging（邮件系统）”，它的原名为 Microsoft Exchange，原本是用于局域网内的一个通信软件，现在是服务器的客户端程序，随着微软操作系统的发展，它已具有强大的功能，但它的主要功能仍为收发邮件。

④ 网络工作组邮局的功能如下：

- 通过 Windows 邮件系统，既可以收发电子邮件，也可以发送、存储和查看所有的电子邮件；
- 使用 Windows 邮件系统还可以组织、访问和共享各类信息，包括联机服务；
- 可以实现局域网、广域网以及邮件的远程访问。

13.2.2　安装和启动邮件服务器

在 NT 网络中，“Microsoft Mail 邮局”就是下面所介绍的“网络工作组邮局”，即通常所说的电子邮件服务器。用户在使用它之前，应当在“邮局端”（即服务器端）和“邮局工作站端”（客户机端）分别进行必要的设置，才能在局域网内使用“网络工作组邮局”的邮件系统收发电子邮件。

设置之后，用户双击桌面上的“收件箱”图标，即可打开“Windows 邮件系统”收发局域网内和 Internet 中的电子邮件。

1. Microsoft Mail 电子邮件系统服务器端的安装和启动

如果在“控制面板”上找不到“Microsoft Mail 邮局”的图标 Microsoft Mail 邮局，请从“（1）安装和启用 Windows Messaging 系统”开始进行；反之，如果已有此图标，则从“（2）设置 Microsoft Mail 邮局”开始执行。

（1）安装和启用 Windows Messaging 系统

安装和启用 Windows Messaging 系统之后，即可启动网络工作组邮局。

① 依次选择“开始”→“设置(S)”→“控制面板”命令选项，在打开的“控制面板”窗口中，选择“添加/删除程序”图标，激活如图 13-1 所示的窗口。

② 在图 13-1 所示的窗口中，选择“Windows NT 安装程序”选项卡，单击“详细资料(D)”按钮，激活如图 13-2 所示的窗口。

③ 在图 13-2 所示的窗口中，选中 Microsoft Mail 选项，单击“确定”按钮，进入安装

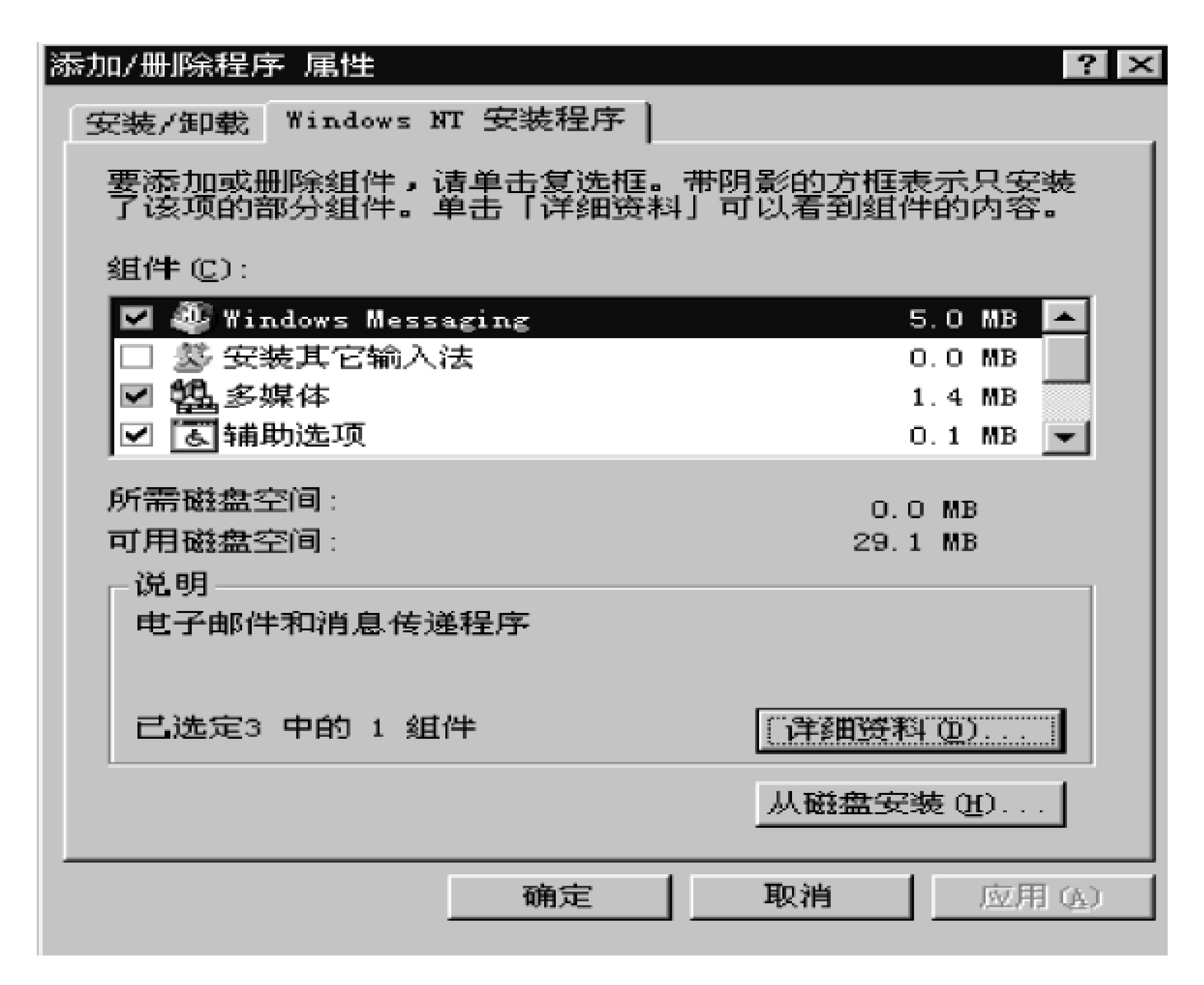


图 13-1 “添加/删除程序 属性”窗口

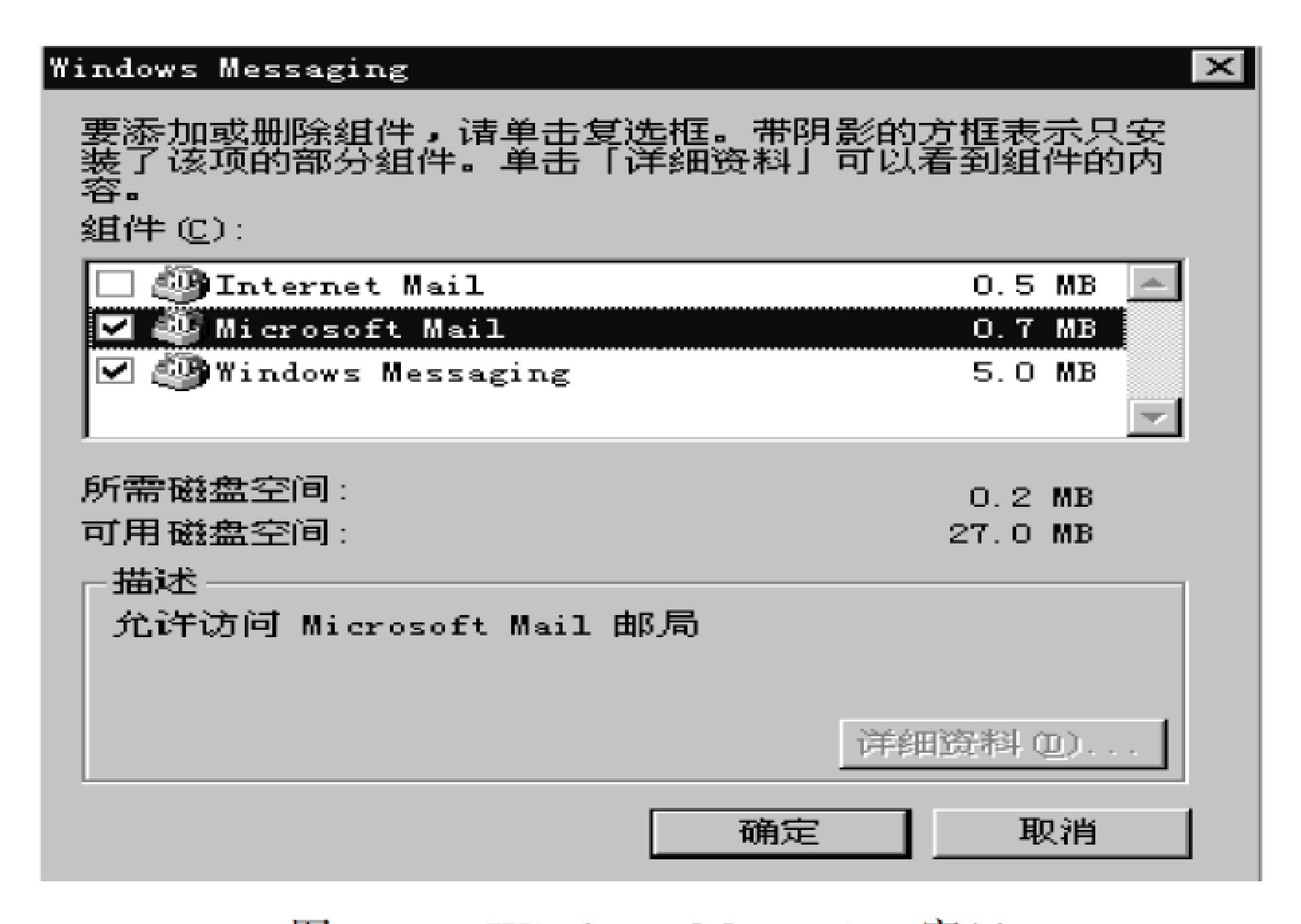


图 13-2 Windows Messaging 窗口

过程。

④ 根据提示，插入所需 CD-ROM 后，单击“确定”按钮。注意，也可以改变源路径或目标路径。例如，选择目标路径为“C:”之后，单击“确定”按钮。

⑤ 复制文件之后，在“控制面板”中便可以找到新增的“Microsoft Mail 邮局”的图标。

(2) 设置 Microsoft Mail 邮局(邮件服务器)

安装和启用工作组邮局“Microsoft Mail 邮局”之后，还需对邮局进行设置。其设置步骤既可以在“本地机”上进行，也可以在“远程机”上进行，设置的主要步骤如下所述：

① 在“邮局端”的硬盘上，建立一个“邮局”目录，例如 C:\mail。

② 使“邮局”目录 C:\mail 共享，以便用来传递电子邮件。对该目录的共享操作既可以在安装之前进行，也可以在安装完成之后进行。

③ 依次选择“开始”→“设置(S)”→“控制面板”命令选项，在打开的“控制面板”窗口中，选择“Microsoft Mail 邮局”图标。

④ 在激活的“Microsoft 工作组邮局管理员”的窗口中，选择创建新的“工作组邮局

(C)”，单击“下一步>”按钮，激活后继的窗口。

⑤ 在激活的下一个“Microsoft 工作组邮局管理员”窗口中，有一个“邮局地点”文本框，首次安装时，可以使用默认地址，直接单击“下一步>”按钮，激活如图 13-3 所示窗口。



图 13-3 “工作组邮局管理员”向导窗口(远程邮局)

⑥ 在激活的窗口中，应键入邮局目录的路径，例如 C:\mail\wgpo0000。如果创建的邮局不在本地机上，可以直接键入邮局目录的远程路径，也可以单击“浏览”按钮，用鼠标选择“工作组邮局”路径，例如，请选择“网上邻居”，并选择远程“工作组邮局”的路径。选择邮局路径之后，单击“下一步>”按钮，激活如图 13-4 所示的窗口。



图 13-4 工作组邮局管理员向导的“输入管理员账号的详细资料”窗口

⑦ 在图 13-4 所示的窗口中，键入有关管理员的详细信息，单击“确定”按钮将分别激活本地工作组邮局和网络工作组邮局返回的信息窗口。

⑧ 最后，单击“确定”按钮，完成“工作组邮局端”的有关设置。

2. Microsoft Mail 电子邮件系统客户端的安装和启动

(1) 安装“Microsoft Exchange”电子邮件系统

Windows 邮件系统用于收发邮件，通过 Windows 桌面上的邮件系统的客户端软件，用户不但可以收取电子邮件，还可以发送、存储和查看所有邮件。

首先检查桌面，如果桌面上没有“收件箱”图标 ，则表示尚未安装 Windows 邮件系统。请选择“控制面板”窗口中的“添加或删除程序”图标，安装 Windows Messaging 中的有关组件。

如果桌面上已有“收件箱”图标，则邮件系统的设置步骤如下：

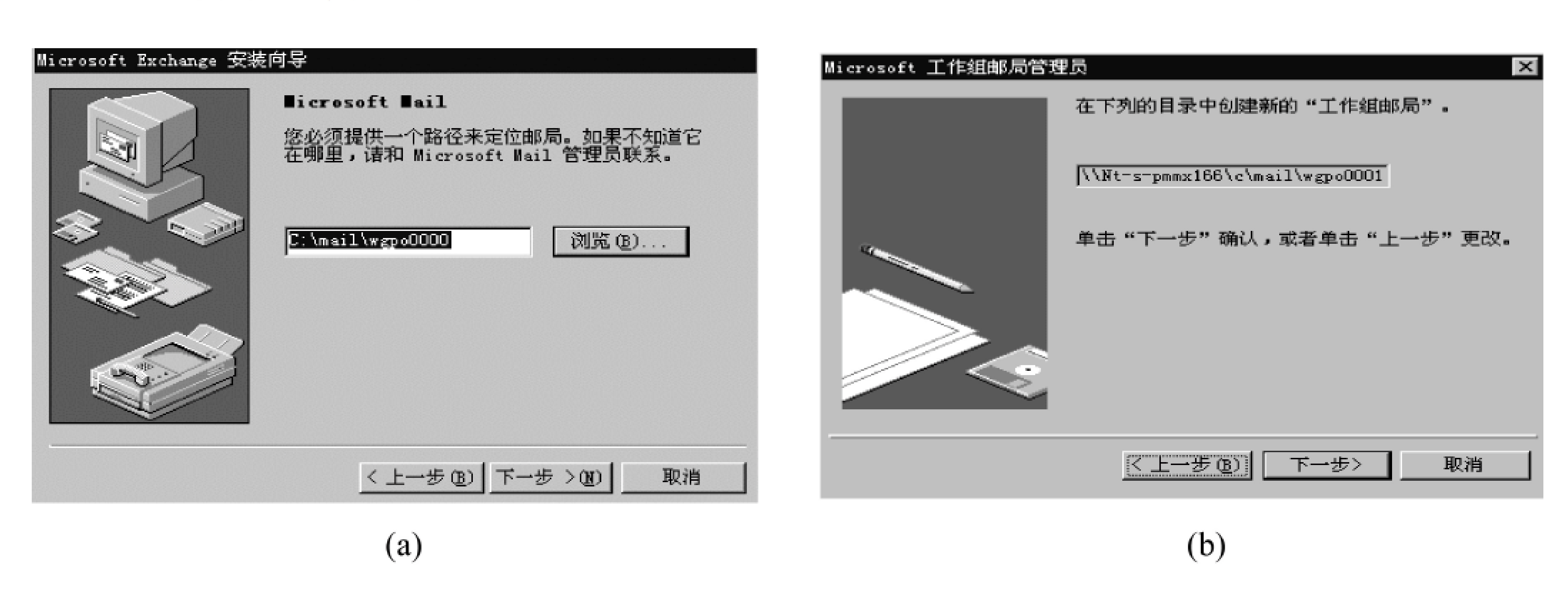
① 在桌面上双击“收件箱”图标，激活如图 13-5 所示的窗口。



图 13-5 “Microsoft Exchange 安装向导”的信息服务选择窗口

② 在图 13-5 所示的窗口中，可以选择 Microsoft Messaging 的配置方式。对局域网邮局用户，选择 Microsoft Mail 方式后，单击“下一步＞”按钮，激活如图 13-6(a)所示的窗口。

③ 在图 13-6(a)所示的窗口中，可以直接键入“网络工作组邮局”的路径，例如，“\\Nt-s-pmmx166\c\mail\wgpo0001”。当然，也可以或直接单击其中的“浏览”按钮，激活图13-6(b)所示的窗口。



(a) (b)

图 13-6 “Microsoft Exchange 安装向导”的邮局定位窗口

④ 在图 13-6(b)所示的窗口中，选择网络工作组邮局的路径。成功之后，单击“下一步＞”按钮，激活如图 13-7 所示的窗口。

⑤ 在图 13-7 所示的窗口中，选择邮局管理员的名称，例如：从列表中选择“郭正昊”，单击“下一步＞”按钮，激活如图 13-8 所示的窗口。

⑥ 在图 13-8 所示的窗口中，输入邮局管理员的口令之后，单击“下一步＞”按钮，激活如图 13-9 所示的窗口。

⑦ 在图 13-9 所示的窗口中，单击“下一步＞”按钮。

⑧ 在随后激活的“安装向导”窗口中，先选择是否将 Exchange 添加到“启动”组中；然



图 13-7 “Microsoft Exchange 安装向导”的邮局管理员选择窗口

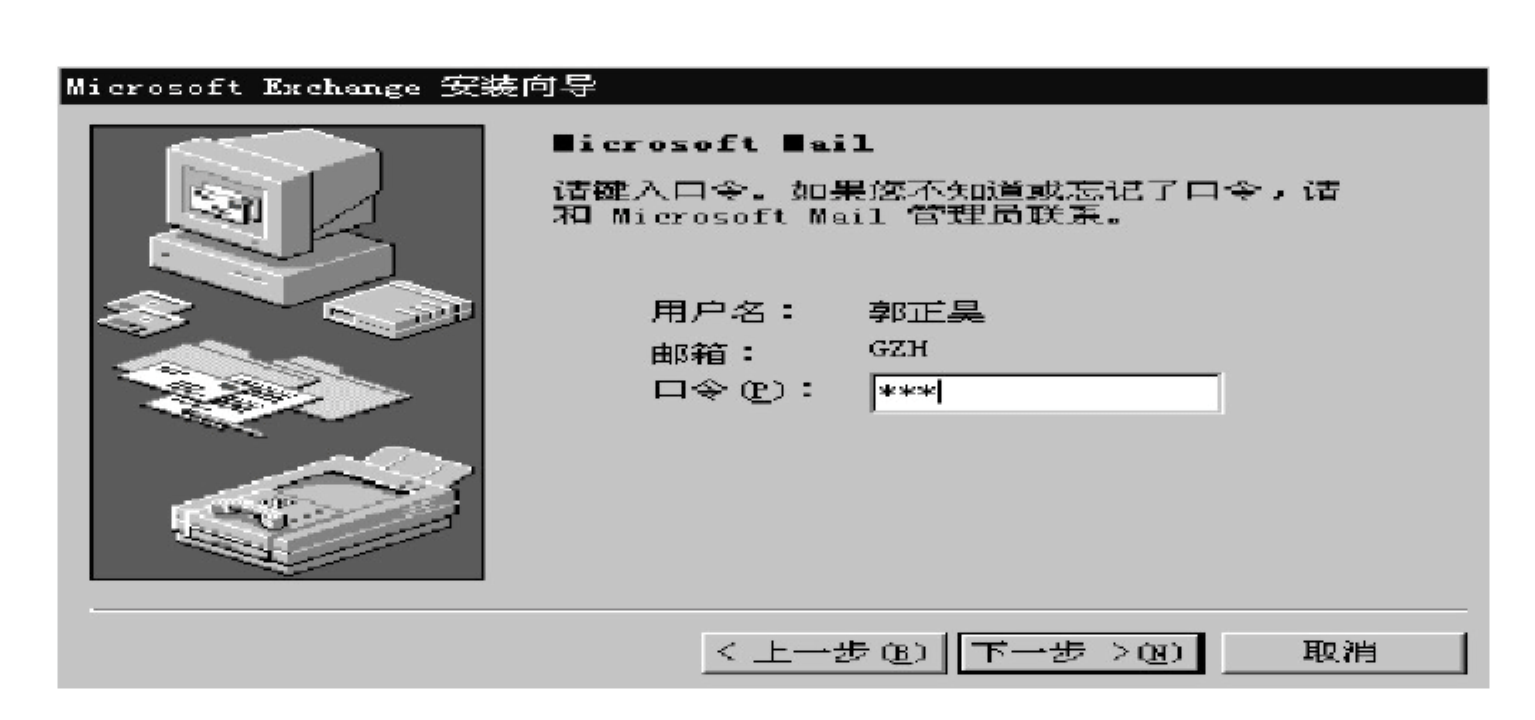


图 13-8 “Microsoft Exchange 安装向导”的邮箱管理员口令验证窗口

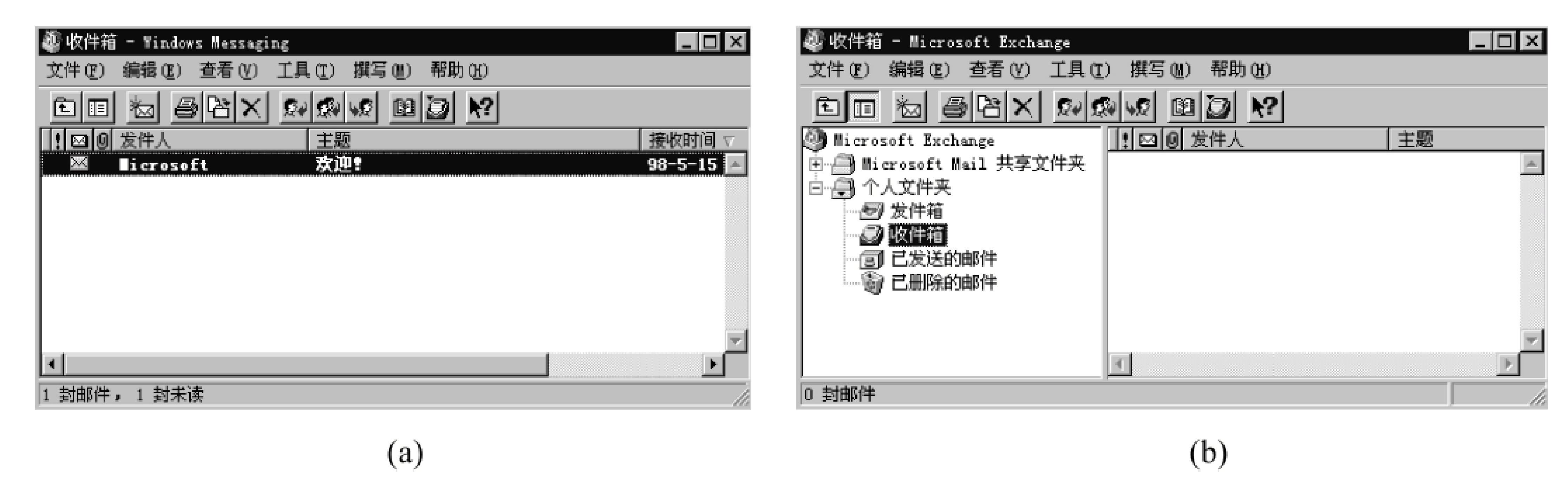


图 13-9 “Microsoft Exchange 安装向导”的个人通讯录路径窗口

后，单击“下一步＞”按钮，激活安装成功的提示窗口。在该窗口中，单击“完成”按钮，激活如图 13-10(a)所示的窗口。

⑨ 在如图 13-10(a)所示的窗口就是邮件系统收发电子邮件时的主要工作窗口。第一次启动时，在收件箱中会显示一封系统内置的欢迎信。

Microsoft Exchange 安装成功之后，用户的 Windows NT 或 95 桌面上便会增加一个“收件箱”图标，以后双击此图标就能启动 Microsoft Exchange。启动后就会出现图 13-10 所示的 Microsoft Exchange 的工作窗口。如果窗口启动后，看不到个人文件夹等部分，可在此窗口中选择菜单“查看”→“文件夹”命令选项；或者双击“个人文件夹”，即可展开其中的内置文件夹名，如图 13-10(b)。此处的文件夹就是信箱。选择并单击信箱名，其右



(a) (b)

图 13-10 “收件箱—Windows Messaging”窗口

边窗口中就会列出该信箱中的全部邮件及其属性。

（2）检查、更改和设置邮件客户端软件 Microsoft Exchange

本地机上的 Microsoft Exchange，在第一次用于收发电子邮件之前必须按下述步骤进行设置。如果用户完成安装之后，发现某些错误致使邮件系统不能正常使用时，也可以按下述步骤进行补救、调整或重装：

① 在图 13-10 所示的窗口中，单击菜单“工具”→“选项(O)”命令选项，将激活如图 13-11 所示的窗口，这就是邮件系统的主要设置窗口，如果系统需要补救、调整、优化或重装系统的设置参数，可选择相应的设置选项卡进行操作，或者直接单击菜单“工具”→“服务(S)”命令选项，激活图 13-11 所示的窗口。



图 13-11 Microsoft Exchange——工具“选项”窗口

② 在图 13-11 所示的“服务”选项卡窗口中，选中“个人文件夹”选项，单击“添加”按钮，激活如图 13-12 所示的窗口。注意：如果不是首次设置，由于个人文件夹已经建立，因此不出现图 13-12 和图 13-13；如果需要修改文件夹，可以单击属性按钮。

③ 在图 13-12 所示的窗口中，键入个人文件夹的文件名，例如 gzh.pst，激活如图 13-13 所示的窗口。

④ 在图 13-13 所示的窗口中，用户可根据需要选择是否加入访问口令。选择后，单击“确定”按钮，激活如图 13-10(b)所示的窗口。

创建/打开个人文件夹文件

搜索(I): mail

wgpo0000

文件名(N): gzh.pst

文件类型(T): PST 文件(*.pst)

打开(O)

取消

帮助(H)

图 13-12　创建/打开个人文件夹窗口

创建 Microsoft 个人文件夹

文件(F): C:\mail\gzh.pst

名称(N): 个人文件夹

加密设置

不加密(C)

压缩式加密(M)

最佳加密(B)

口令

口令(P):

确认口令(V):

将口令保存在口令清单中(S)

确定　取消　帮助(H)

图 13-13　创建 Microsoft 个人文件夹窗口

(3) 启动 NT"Microsoft Mail 邮局"客户机

建立邮局之后,邮局工作站上的 Microsoft Exchange 在第 1 次用于收发电子邮件之前还必须按下述步骤进行设置。如果用户完成设置之后,发现某些错误致使邮件系统不能正常使用,也可以按下述步骤进行补救、调整或重装。启动"Microsoft Mail 邮局"客户机工作站的设置步骤如下:

① 在图 13-10 所示的窗口中,选择"工具"→"选项(O)"命令选项,激活如图 13-11 所示的窗口。该窗口是邮件系统设置的主要窗口,也是系统需要补救、调整、优化或重装系统时设置参数的界面。在窗口中,用户可选择需要设置的选项卡进行操作。

② 在图 13-11 所示的窗口中,选择"服务"选项卡后,选中 Microsoft Mail 选项后,单击"属性"按钮,将激活 Microsoft Mail 窗口,在该窗口可以对其属性进行设置或修改,例如,修改邮局的连接路径。

(4) "Microsoft Mail 邮局"客户机上的"收件箱"窗口

在图 13-10(b)的窗口中,只需将鼠标移到工具条按钮上,片刻就会显示出其相应的

名称。为了帮助读者用好工具条按钮，下面按从左至右的顺序，依次列出各工具按钮的中英文对照名称及用途。常用的按钮有：上一级 Previous、文件夹 Folder、新邮件 New Mail、打印 Print、移动邮件 Move Mail、删除 Delete、答复发信人 Reply Author、全部答复 Reply All 和帮助 Help 等按钮。单击这些按钮，均能调出相应的窗口。

13.3 网络邮局的管理

13.3.1 启动“邮局管理程序”

邮件服务系统建立之后，邮局管理员可在网络的任何计算机上使用“邮局管理程序”对网络邮局进行管理。常见的邮局管理工作有添加、删除和管理邮局用户账号等。

启动“邮局管理程序”的步骤如下：

① 选择“开始”→“设置(S)”→“控制面板”命令选项，在打开的“控制面板”窗口中，选择“Microsoft Mail 邮局”图标，激活后继的窗口。

② 在激活的“Microsoft 工作组邮局管理员”的窗口中，选中“管理现有的工作组邮局(A)”单选项后，单击“下一步＞”按钮。

③ 在激活的“Microsoft 工作组邮局管理员”窗口中的“邮局地点”文本框中，输入现有的工作组邮局的路径，如果已知所要管理的邮局路径，可直接键入地址。否则，可以单击“浏览”按钮，激活后继的“浏览邮局”窗口。

④ 在激活的“浏览邮局”窗口中，可以选择现有的工作组邮局的路径，例如，使用鼠标选中“本地邮局”或“网络邮局”中的 wgpo000 后，单击“确定”按钮。

注意：系统上可能存在多个工作组邮局，因此，邮局管理员应当清楚需要管理的是哪个邮局，其中有多少邮件账号。

⑤ 在出现图 13-14 所示的窗口时，应确认邮局路径是否正确，之后可单击“下一步＞”按钮，激活如图 13-15 所示的窗口。否则，单击“＜上一步(B)”按钮，返回上一个窗口进行修改。



图 13-14 “工作组邮局管理员”管理向导的邮局地址确定(远程邮局)窗口



图 13-15 “工作组邮局管理员”管理向导

⑥ 在图 13-15 所示的窗口中,需要先输入网络邮局管理员所要管理的邮箱名称和该邮箱的口令。输入之后,单击“下一步>”按钮,经系统确认正确后,激活如图 13-16 所示的窗口。否则,单击“<上一步(B)”按钮,返回上一个窗口进行修改。



图 13-16 “邮局管理程序”窗口

⑦ 图 13-16 所示的窗口是邮局管理员进行管理工作的主要界面。至此,启动“邮局管理程序”的操作完成。该窗口显示了该邮局内现有用户的清单。

13.3.2 使用“邮局管理程序”进行管理

邮局管理员使用“邮局管理程序”管理网络邮局,主要包括添加或删除用户及查询、修改所选邮局用户的各种信息等内容,例如,更改邮箱名称、用户姓名、口令和电话号码等。

1. 添加新用户

添加新用户的步骤如下:

① 在图 13-16 所示的窗口中,单击“添加使用者(A)”按钮,激活如图 13-17 所示的窗口。

② 在图 13-17 所示的窗口中,输入用户的有关信息。其中,姓名、邮箱和口令是管理员必须填入的,其他信息可根据实际情况酌情输入。最后,单击“确定”按钮,返回如图 13-16 所示的窗口。

添加用户

姓名(N)：李力
邮箱(M)：lili
口令(P)：lili
电话#1：64961155-1234
电话#2：64073337
办公室(O)：234
部门(D)：实验中心
附注(T)：实验中心副主任

确定　取消

图 13-17　“添加用户”窗口

2. 修改用户信息

修改用户信息的步骤如下：

① 在图 13-16 所示的窗口中，选择所要修改的用户名后，单击“详细资料(D)”按钮，激活与图 13-17 类似的所选用户的信息窗口。

② 在用户的信息窗口中，可以选择修改、查看该用户的各种信息。修改之后，单击“确定”按钮，返回如图 13-16 所示的窗口。至此，“修改用户信息”的操作完成。

3. 删除邮件账号

在图 13-16 所示的窗口中，先选择所要删除的邮件账号名，再单击“删除使用者(R)”按钮，激活电子邮件的“用户删除确认”窗口。为避免误删除，应当进行仔细的核对，最后，单击“是(Y)”按钮，确定选择了删除操作，返回图 13-16 所示的窗口。至此“删除邮件账号”的操作完成。

13.4　电子邮件系统客户端软件的使用

对网络管理员来说邮局工作站上的主要工作是为用户编辑、发送和接收电子邮件做好准备。对于邮局用户来说则是如何使用客户端的软件。例如：对于 Micorsoft Exchange 的用户，首先，应掌握如何编辑新邮件，特别要掌握邮件头的填写、正文的编辑以及贴附现成文件的方法；其次，就是如何将写好的邮件发送出去。

1. 启动电子邮件系统客户端软件—Microsoft Exchange

前面已经讲过，如果桌面上没有“收件箱”图标，则可能未安装 Windows 邮件系统。应使用“添加或删除程序”安装有关组件。当桌面上已有“收件箱”图标时，可以在桌面上双击“收件箱”图标，激活如图 13-18 所示窗口，正确输入口令之后进入如图 13-10 所示的 Microsoft Exchange 工作窗口。如果不想每次输入“口令”，可选中“记忆口令(R)”选项。

2. 发送与接收电子邮件

在 Microsoft Exchange 投入使用之前，首先应该检验它的收发工作是否正常。通常的检验办法是发一封测试信给自己收。使用 Microsoft Exchange 收发电子邮件的操作包括以下几种：

(1) 发送(传送)电子邮件



图 13-18　进入“Microsoft Mail”工作窗口时的对话窗口

发送(传送)电子邮件之前，应先将邮件编辑好，再发送到“发件箱”中，最后进行传递和接收邮件等操作。发送邮件的步骤如下：

① 先在 Microsoft Exchange 新邮件编辑窗口中编辑好邮件，然后，单击工具栏最左边的“发送(S)”按钮，便会把邮件发送到“发件箱”待发，随后返回 Microsoft Exchange 的主工作窗口。

② 在 Microsoft Exchange 的主工作窗口中，选择“工具”→“传递方式(D)”→“Microsoft Mail(局域网邮件)”或“Internet Mail(Internet 邮件)”命令选项后，Microsoft Exchange 才会做一次相应的发送“发件箱”中信件的操作，这样可以大大节约上网时间及费用。

(2) 接收电子邮件

由于 Microsoft Exchange 在图 13-10 所示的窗口中，选择“工具”→“传递方式(D)”→Microsoft Mail 或 Internet Mail 命令选项后，才会同时做一次收、发电子邮件的操作，所以如果用户的电子邮件服务器很快，那么在发送信件的同时，也将收到发给自己的信件。如果用户收到的不是自己发给自己的信件，而是系统管理员发来的信，则说明发送信件的操作可能失败了。

13.5　在 Windows 98 上启用网络工作组邮局

微软公司从 Windows 3.11 起开始提供 Microsoft Mail 工作组邮局的支持，因此，对于使用 Windows 95/97/NT 及以前版本系统的用户可以按照本书前面各节中的步骤直接建立起电子邮件系统。而对于使用 Windows 98 建立电子邮件系统的用户，则应当按照下述步骤进行工作组邮局的补充安装：

① 插入 Windows 95(97)光盘，找到\Pwin95(97)目录。

② 将 precopy1.cab 和 precopy2.cab 复制到硬盘的某一个目录下。

③ 使用 WinZip.exe 或者 WinRar.exe 进行解压操作。

④ 依次选择“开始”→“设置(S)”→“控制面板”命令选项，在打开的“控制面板”窗口中，双击“添加/删除程序”图标，在激活的窗口中，选择“Windows 安装程序”选项卡，如图 13-19 所示。

⑤ 在图 13-19 窗口中，单击“从磁盘安装”按钮，在激活的窗口中，选择 precopy2.cab



图 13-19　控制面板中的“添加/删除程序”窗口

解压程序所在的目录，如图 13-20 所示。



图 13-20　“打开”解压文件所在的目录窗口

⑥ 在图 13-20 所示的窗口中，选择 precopy2.cab 解压程序所在的目录后，单击“确定”按钮，出现图 13-21 所示的窗口。

⑦ 在图 13-21 所示的“从磁盘安装”窗口中，选择 Microsoft Exchange 复选项后，单击“安装”按钮，系统将从 Windows 95 光盘上复制所需要的文件，当出现“版本冲突”窗口时，单击“是”按钮，保留原有的文件。文件复制结束后，重新启动计算机，完成在 Windows 98 上补充安装 Microsoft Mail 邮局的过程。

在 Windows 98 中，再次打开“控制面板”窗口时，可以看到新增的 Microsoft Mail 邮局图标，同时在桌面上会出现一个“收件箱”的图标。以后的步骤依然为配置和管理邮件服务器(即工作组邮局)和客户机上作为客户端软件的“Microsoft Exchange 的收件箱”两个主要部分，请参照 13.3～13.4 节进行。



图 13-21 “从磁盘安装”窗口

习题

(1) 电子邮件系统的主要功能有哪些？由哪几部分组成？

(2) 电子邮件系统中常用的服务器端软件有哪些？客户工作站端软件有哪些？

(3) 什么是“网络邮局”？它应有具有哪些主要职能？

(4) Windows NT 局域网邮件服务器(工作组邮局)的建立步骤有哪些？

(5) 当需要建立或管理的邮件服务器(工作组邮局)不在本地机上时，建立和管理工作组邮局的操作步骤与在本地机上相比有何异同？

(6) 如果“控制面板”窗口中，如果找不到“Microsoft Mail 邮局”的图标说明了什么？应如何解决？

(7) 在使用 Windows 95/NT 工作站时，如果桌面上没有“收件箱(In Box)”图标说明了什么？应如何解决？

(8) 如何安装、检查和更改 Microsoft Mail 的设置？

(9) 如何安装、检查和更改 Microsoft Exchange 的设置？

(10) 如何管理 Windows NT 邮件服务器(工作组邮局)中的邮件账号？管理的内容有哪些？

(11) 在局域网的非本地机上，应如何管理局域网邮件服务器(工作组邮局)中的用户？

(12) 什么是电子邮件？在办公自动化中它扮演了什么角色？

(13) 如何在 Windows NT 邮件系统工作站上发送电子邮件？

(14) 如何在 Windows 95/NT 邮件系统工作站上发送电子邮件？

(15) 怎样传递文本、图形或其他类型的邮件？

(16) 如何在 Windows 98 上安装电子邮件系统？服务器端和客户工作站端应进行哪些设置？

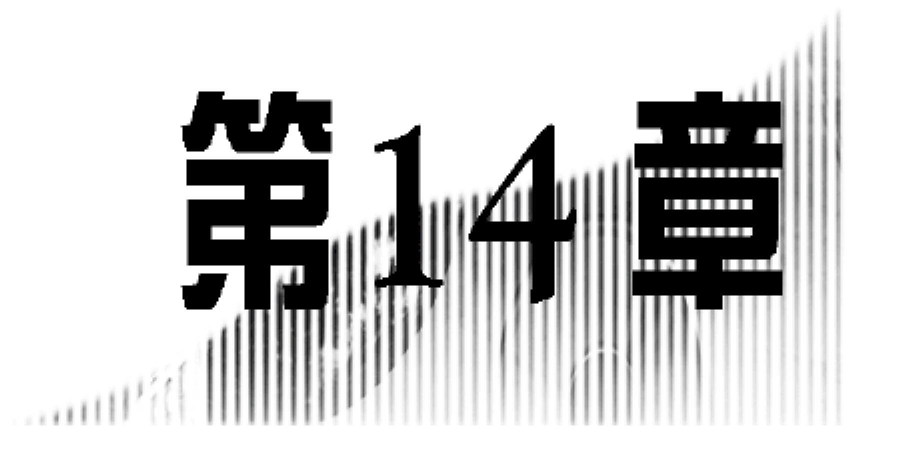
实训题目

1. 在 Windows NT Server 或者 NT Workstation 计算机上，建立、设置和管理局域网的邮件服务器（工作组邮局）。

2. 在各种 Windows NT 工作站上管理局域网的邮件服务器（工作组邮局）。例如，添加、修改某用户账号中的信息。

3. 启动、设置和使用局域网内各种“邮局工作站”的电子邮件功能，并使用客户的“收件箱”编辑和收发电子邮件。

4. 在 Windows 98 上补充安装电子邮件系统，并设置、使用和管理局域网的工作组邮局。



第14章 数据保护与系统恢复技术

本章将介绍网络日常管理中的基本数据保护以及系统维护的概念和技术。其中包括网络中的数据保护、NT 系统数据保护与系统修复中的基本概念和基本方法，以及网络管理员应掌握的数据保护和系统修复技术。

主要内容：

- 网络中的数据保护的基本概念和基本方法；
- 网络系统中数据备份程序的应用实例；
- Windows NT 中的备份程序；
- 容错与 NT 中的容错技术；
- 利用“上一次的正确系统配置”的环境恢复 NT 系统；
- 利用“紧急修复磁盘”修复被损坏的 NT 系统；
- 利用“注册表(registry)”修复被损坏的 NT 系统；
- 利用“NT 启动磁盘”修复被损坏的 NT 系统。

14.1 网络中的数据保护

设计一个实用的局域网管理系统时，必须考虑和解决好数据保护的问题，在网络的设计和运行中，需要设计的与数据保护相关的系统有：网络数据备份系统、网络数据恢复系统和网络灾难恢复系统。

14.1.1 数据保护概述

网络管理员必须对网络数据保护的重要性、网络备份的种类、备份设备、存储介质，以及备份的基本方法和备份制度等有很深的了解，并且制定出目标明确的备份计划和实际可行的恢复手段。

1. 网络中数据保护的重要性

在实际的网络运行环境中，网络中数据资源的保护是十分重要的。因为，硬件与系统软件的损害可以通过重新购置，或重新安装等方法进行补救，而系统的数据资源却是众多

企业多年积累的结果，它是企事业单位的“生命”，一旦失去，可能造成永远也无法弥补的损失。历史上就出现过由于系统损坏，数据丢失而导致公司破产的例子。因此，系统管理员必须充分地认识到以下几点：

① 企事业、公司的信息和数据就是他们的利益和财富。

② 数据的备份是十分重要的，也是网络管理员日常最重要的工作之一。

③ 任何一个实用的网络应用系统的设计中，必须具有网络数据备份、数据恢复、发生灾难时的恢复计划和具体措施等。

2. 网络中数据定期备份的原因和目的

基于网络数据的重要性，网络中的文件和数据需要定期备份。备份的目的是为了在数据和系统损坏之后能够迅速地恢复文件、系统或数据。制作备份的原因综述如下：

① 防止数据文件的意外删除；

② 防止恶意员工或非法入侵者的破坏；

③ 防止硬盘或其他媒介的物理故障。

3. 在设计网络文件与数据备份系统时需要考虑的因素

网络系统管理员在设计备份方法时一定要考虑到，并能够回答以下问题：

① 一旦系统遭到破坏，需要多长时间可以恢复系统；

② 怎样备份数据才可能在恢复系统时损失最小。

14.1.2　网络数据文件备份系统

本小节讨论网络数据文件备份系统实施的基本过程。

1. 建立数据文件备份的策略

在具体实施整个网络的数据保护计划之前，确定数据保护的策略和方法是十分必要的。最保险的方法是备份计算机上所有的数据资源，然而，这是不切实际的。因而，在建立备份之前，必须考虑和解决好以下几个基本问题：

① 备份间隔　多长时间间隔做一次备份。

② 备份内容　应让用户及时地了解到服务器和工作站备份的区域与备份的内容。

③ 备份能力　备份系统硬件和存储介质可提供的最大储存能力。

④ 备份时间的选择　备份时间段的限制。例如是否必须在低负荷时进行备份等。

⑤ 备份的所在地　例如是本地存储还是异地存储，本地存储恢复速度快，但对本地设备的物理损坏无能为力；异地存储可以防止自然灾害、人为破坏和设备的物理损坏。

2. 备份设备与存储介质的选择

在选择备份设备时，应充分考虑到网络文件系统的规模，以及需要进行备份文件的重要程度。过去，备份设备的种类较少，价格较高，大型单位的存储设备一般为磁带机和磁性存储介质，例如磁带、硬磁盘、磁鼓等。

目前，随着网络硬件和计算机技术的发展，应用软件的体积日趋庞大，需要交换和存储的数据量越来越大，这在某种程度上也促进了现代硬件设备的进步和改进，可选择的设备种类和方案也越来越多。一般的网络操作系统都支持多种不同的硬件接口，例如串行口、并行口、IDE 口、USB 口、SCSI 接口等，因而，常见的服务器大都支持磁带、MO（磁光

盘）、高容量软盘驱动器、活动硬盘、光盘等多种可移动存储设备，其对应的自然存储媒介也有多种选择。作为网络服务器来说，SCSI 接口的设备应当说是最佳的选择。

一般来说，磁介质具有可靠、廉价和可移动性强等特点，常作为网络的存储介质。不同移动存储设备的特点各不相同，现在归纳如下：

（1）ZIP、LS-120 等大容量软驱

① 由于使用方便，因此，普及率较高，数据的通用性较好。

② 读写速度慢。

③ 盘片易损坏，可靠性较差。

④ 存储容量有限。

总之，ZIP 和 LS-120 等大容量软驱适用于移动办公、快速简单的归档备份以及存储量较大的扫描或注册表文件、下载文件和电子商务数据的短期存储等场合。

（2）活动硬盘驱动器

① 读写速度快。

② 容量大。

③ 便携性好。

④ 价格高，导致普及率较低。

活动硬盘被广泛地应用于数据备份、音频/视频等巨型文件的存储、大量的扫描文件的归档备份和整个系统的整体备份等场合。

（3）CD-R/CD-RW 光盘驱动器

① 读写速度较快。

② 容量较大。

③ 便携性好。

④ 极低的价格，普及率极高，数据的通用性较好。

CD-R/CD-RW 光盘驱动器自进入计算机市场以来，凭借其低廉的价格和极高的性能价格比，得到了迅速的发展和普及。现在它不但为广大普通用户所青睐，也被广泛地应用于数据备份、巨型文件的备份和存储、大量的扫描文件的归档备份和整个系统的整体备份等多种场合。

（4）磁带机

① 读写速度中等。

② 容量较大。

③ 寿命长。

④ 价格较高，普及率低，数据的通用性较好。

⑤ 备份和恢复时使用不便。

磁带机通常用在较大规模网站、企业和网络的整体备份、大型数据库等巨型文件的归档备份和高阶工作站的整体备份等场合。如果磁带机能够进一步降低价格、提高传输速度、统一标准的话，就能在更大的范围内得到推广和使用。

（5）正在发展的其他设备

① DVD-ROM 正在取代光驱的位置，将成为下一代光盘的事实上的标准。

② MO(磁光介质的记录设备)是磁、光相结合的存储设备,它具有活动硬盘的全部优势。

③ 半导体存储卡。如 MP3 随身听、MS 存储棒、CF(小型快闪)卡、Smart Media(智能媒体)卡和 MMC 卡等多种存储设备正在以日新月异的速度发展着。

常见移动式存储设备及其介质的特点参见表 14-1。

表 14-1　数据文件的交换设备—常用移动式备份存储设备及其所用介质的特点

移动式存储设备	存储媒介名称	存储容量	速度	价格	适用场合	使用特性
大容量软盘驱动器	高容量软盘(Zip、LS-120)	低 100M	极低速	极低	少量数据的归档备份	不可靠
磁带机(SCSI)	数字磁带(4mm/8mm)	较高	传输速度较慢	适中	服务器和工作站的日常备份	使用不便、存储寿命长
数字磁带机	数字线性磁带	高	高速	高	企业备份	使用不便、存储寿命长
活动硬盘驱动器(SCSI 或 IDE)	活动硬盘	大	高速	高	服务器(SCSI)和工作站(IDE)的整体备份	较可靠、存储寿命长
CD-ROM 光驱	只读光盘(CD-ROM)	中	低速	低	频繁访问文档、软件的归档,分区和硬盘的整体备份	较可靠,便于携带、仅能使用一次
CD-RW 光盘刻录机	可读写光盘(CD-RW)	中	低速	中	频繁访问的文档和软件	较可靠,便于携带、能使用多次、使用方便

目前,一般大、中型企事业单位的应用系统中,可以采用的存储介质有 CD-R/CD-RW 盘、磁带和活动硬盘等。其中:CD-R/CD-RW 盘和活动硬盘具有高容量、高可靠性、保存周期长、易于保存和恢复等优点,是大、中、小型单位均适用的备份介质。

一般中、小型单位的应用系统可以根据自己的实际情况和能力,选择高容量软盘、CD-R/CD-RW 盘和活动硬盘等多种存储介质。其中的 CD-R/CD-RW 盘和活动硬盘具有高容量、可操作性强、价格和可靠性适中等特点,是中小型单位的首选备份存储介质。

3. 确定备份程序

备份程序可以选择局域网使用的网络操作系统中的内置功能程序,也可以选择使用第 3 方开发的备份程序。在选择第 3 方备份程序时,应注意以下几个问题:

① 备份程序所支持的网络操作系统类型。

② 备份程序支持的备份设备和存储介质的类型。

③ 备份设备所处的位置。例如,备份设备是安装在服务器上还是在工作站上。

④ 当网络中存在多个备份服务器时,可否在其中的一个备份设备上完成这多个备份服务器的备份操作。

实例：对于使用 Windows NT 网络操作系统的小型公司网络来说，服务器和工作站本身的引导分区和数据分区的信息，可以采用第 3 方的 Ghost.exe 程序进行分区的克隆备份(即整体备份)。该程序可以从 DOS、Windows 和 CD-ROM 上引导和运行。备份之后的程序可以存放在硬盘上，也可以采用刻录机进行刻录。为了防止不测事件，刻录后的 CD-R 和 CD-RW 盘片应异地存放。使用此种方法备份 2GB 的数据分区，在系统分区恢复时，只需要 20 分钟左右的时间。每个 CD-ROM 盘片的价格也很低，只有 2 元～5 元。总之，使用 Ghost.exe 程序进行系统和数据的备份，具有使用设备价格低廉(600 元～3 000 元)、方法简单、可靠性较高、恢复时间短，成本低等优点，因此，很适合中小单位的网络或单机系统备份和恢复时使用。而对于用户指定的数据文件则可以选择 Winzip.exe 和 Winrar.exe 进行备份。

4. 建立备份制度

备份文件通常是指将日常维护工作所必须保护的系统或应用数据文件存储(复制)到指定的介质上，以备发生不测时，完成系统或数据的恢复。常用备份文件的类型如下所述：

- 整体备份(full backup)　又称常规备份或普通备份(normal backup)，即存储所选分区的所有文件。例如：克隆某个分区，就属于这种类型。
- 差量备份(differential backup)　存储上一次整体备份以来的所有文件。
- 增量备份(incremental backup)　存储上一次整体备份或增量备份以来的所有用户修改过的文件。
- 日常备份(daily backup)　存储每天修改的文件。
- 归档备份(archive backup)　又称复制备份(copy backup)，即存储所有被选择的文件，而不管其他文件。例如，使用常用的压缩软件 winrar.exe 就可以完成归档备份和增量备份。

图 14-1 说明了 3 种备份类型的差异。在进行以上 3 种备份类型的备份时，增量备份比差量备份要快；但使用磁带恢复时，增量备份比差量备份所用的时间长。这是因为增量备份恢复时，需要整体备份和每次的增量备份，而磁带属于顺序存储设备，因此，所需时间就较长。差量备份在备份时，在每个备份上都需要存储更多的数据，但恢复时，只需要整体备份和最后一次的差量备份。在系统调试好之后，管理员一般应先做一次完整的数据备份，以后，再根据制定的备份制度执行某种类型的备份操作。

(1) 备份版本的数量

较大单位的网络管理员，对于含有重要数据的文件，通常使用(3～4)个备份版本。对于一般性保护的文件，至少不能少于 2 个备份。

(2) 备份的存放位置

较大单位的网络管理员，对于含有重要数据的多个备份，应当异地、安全存放。例如：对于上述的 3～4 个备份版本，应当至少存放在 2 处以上的安全地方。

(3) 备份工作的执行者和工作日志

再好的备份制度，没有落实执行者也等于零。因此，在多个网络管理员中，应明确各种备份工作的执行者，并建立好交接班的维护及备份等工作的工作日志。

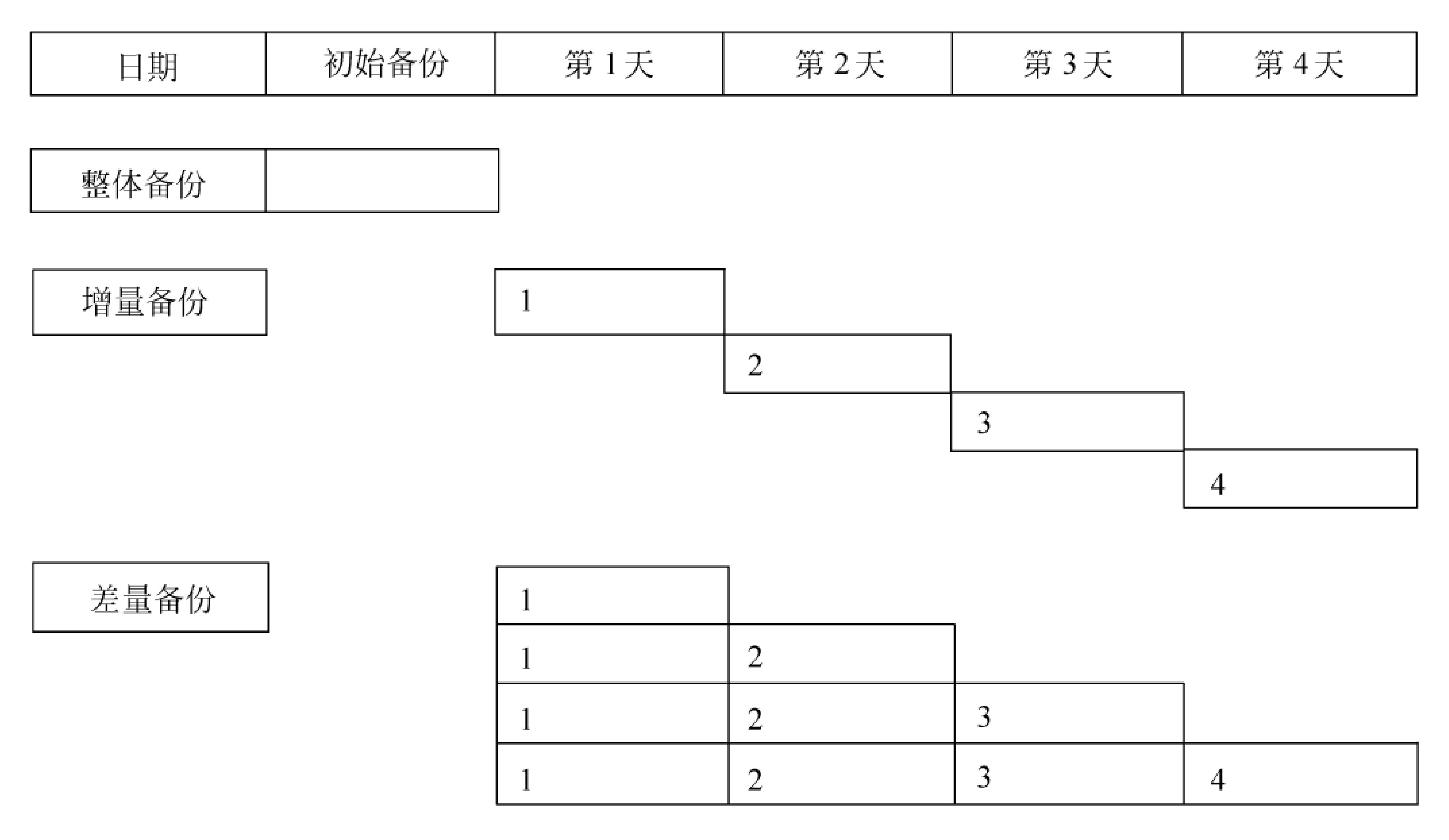


图 14-1　整体备份、增量备份和差量备份

(4) 备份计划的具体内容

用户在做备份计划时,应当包括下述基本内容:

① 需要备份的数据量。

② 根据每天、每周和每月修改的数据量的大小,来确定相应的备份内容和备份时间间隔。

③ 确定可使用的备份存储空间(容量)大小。

④ 拟备份的数据类型,例如,是操作系统、应用程序还是用户数据。

⑤ 备份数据的位置。例如,是用户本地计算机的数据,还是服务器上的数据。

⑥ 备份版本的数量和存放地点。

⑦ 备份工作的责任人。

实际上,制作备份制度计划表时,最主要的就是选择需要备份文件的内容和备份的时间周期,及其使用的存储设备和介质。

例如,某公司所做的备份计划如下:

- 每月做一次　系统分区的整体备份,使用光盘和磁带存储。
- 每周做一次　网络数据库文件和网络用户账号与属性的差量备份,使用磁带和硬盘存储。
- 每日做一次　从上次备份以来用户修改过文件的增量备份,使用磁带和硬盘存储。
- 备份的数量　每种备份做好制订数量的备份。例如,使用 3 盘磁带或活动硬盘循环存储。
- 按特定用户对数据保护的要求　做好指定数据的 3 个归档备份,使用活动硬盘和光盘存储。
- 存放位置　将各备份分别存放在两个不同的安全地带。

• 备份中的其他问题　如备份责任人员、核查人员和备份工作的交接班日志等。

由于备份的目的是为了恢复，所以网络管理员应当非常明确，并且可以随时告知用户有关系统或数据恢复方面的问题，其中最主要的是提供恢复时间和恢复内容两方面的信息。例如：系统破坏后，正常情况下，1 小时内可以恢复主引导区内的所有数据和文件。

14.2　网络备份程序应用实例

下面以小型公司网络为例，来说明备份程序的具体应用和执行步骤。

1. 引导分区的整体备份

本案例使用 NT 为网络操作系统，利用第 3 方程序 Ghost.exe 对所选分区或整个硬盘进行整体备份时的主要步骤如下：

① 首先应当在 Windows NT Server（服务器）和 Windows 98/2000（客户工作站）的计算机上安装 Ghost 程序。

② 在 DOS、Windows 和 CD-ROM 上引导之后运行此程序。

③ 对所选分区或整个硬盘进行整体备份，俗语为克隆分区或克隆硬盘。

④ 整体备份之后，将生成上述分区或硬盘的整体备份文件的映像文件。该文件可以存放在本地硬盘的其他分区、活动硬盘或光盘上。

⑤ 制作映像文件的备份。例如：当整体备份的是分区时，可以使用刻录机，即 CD-RW 或 CD-ROM 等设备，刻录映像文件的备份，以便存放。

⑥ 根据需要制作预定数量的整体备份副本。

⑦ 刻录的光盘、活动硬盘及其副本等，应按照预定的计划异地存放，以备不测。

⑧ 首次使用上述备份设备进行系统或硬盘的备份后，应使用所制作的备份进行备份数据的恢复措施，以检测副本的可用性和恢复的完整性，同时还可以确定恢复所需的时间。例如：使用上述方法备份 2GB 的数据分区，系统分区恢复测试时，需要 20 分钟左右即可恢复原有分区中的所有内容。

2. 使用 Ghost.exe 程序进行系统数据的备份

使用 Ghost.exe 程序进行系统数据备份的具体步骤如下：

(1) 安装 Norton Ghost 2001

① 将具有 Ghost.exe 程序的安装光盘放进 CD-ROM。

② 在激活的“安装 Norton Ghost 2001”的选项窗口中，选择“安装 Norton Ghost 2001”选项，可以进入安装向导窗口，跟随安装向导即可完成安装过程。

(2) 制作 DOS 下运行的 Norton Ghost 2001 的启动恢复盘

由于在 DOS 下运行 Norton Ghost 2001 可以获得最佳的效果，因此，首先应该在 Windows 98/NT 下，创建一张可以在 DOS 下启动的 Ghost 引导盘。操作步骤如下：

① 依次选择“开始”→“程序”→“Norton Ghost 2001”→“Norton Ghost 启动向导”命令选项，激活如图 14-2 所示的窗口。

② 在图 14-2 所示的窗口中，可以有两种选择，图 14-2(a)为制作支持对等网的启动

盘,图 14-2(b)为制作支持 CD-ROM 的启动盘。如果用户打算制作单个计算机的整体备份,请选择后者。



(a) (b)

图 14-2 创建“Norton Ghost 引导盘”的类型选择窗口

③ 选择之后,单击“下一步”按钮,激活如图 14-2 所示的窗口。

④ 在图 14-3 所示的窗口中,可以直接单击“下一步”按钮,激活如图 14-4 所示的窗口。

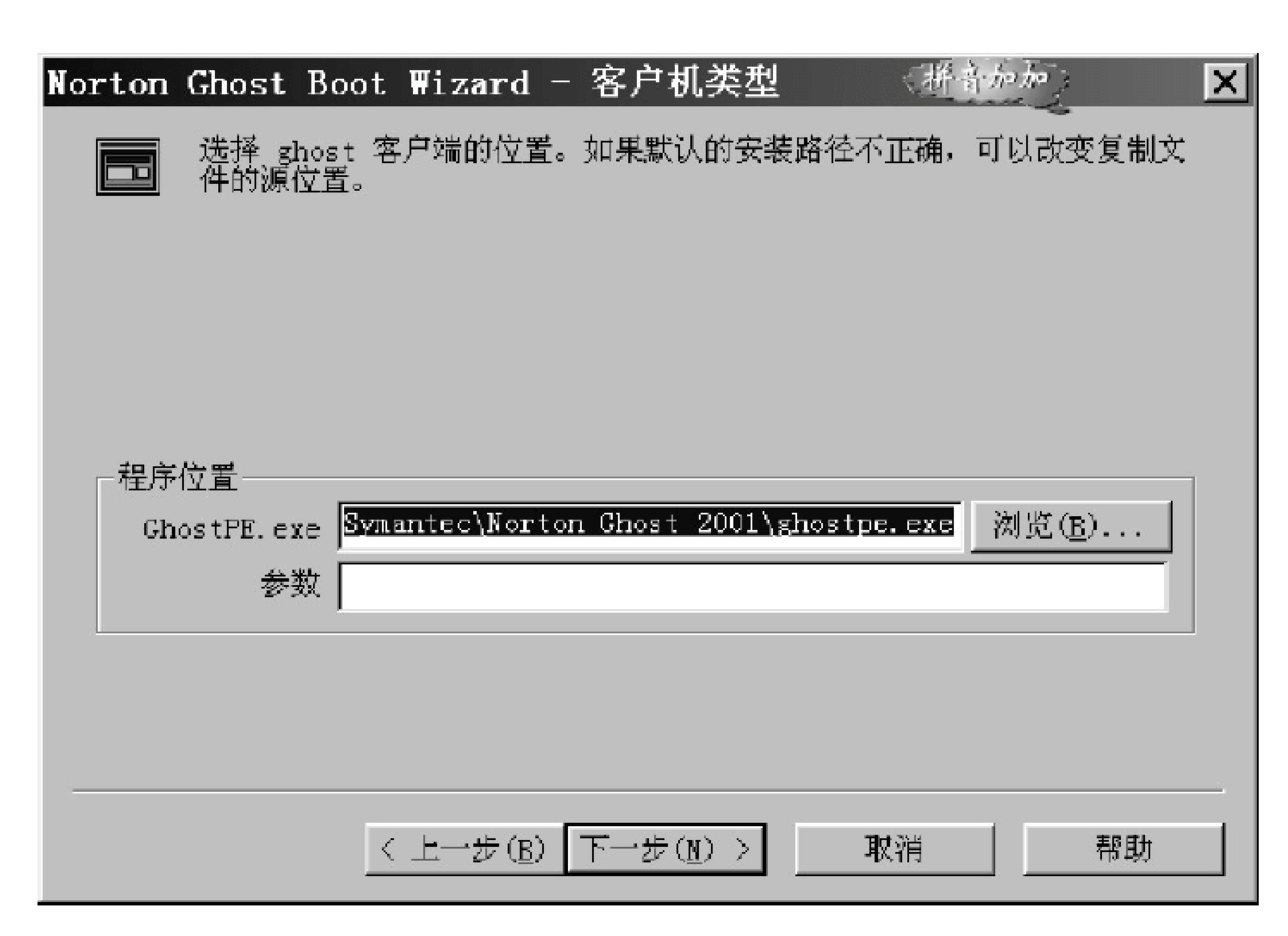


图 14-3 创建“Norton Ghost 引导盘”向导窗口的程序定位窗口

⑤ 在图 14-3 所示的窗口中,可以直接单击“下一步”按钮,激活如图 14-4 所示的窗口。

⑥ 在图 14-4 所示的窗口中,插入用于在 DOS 下启动的软盘后,单击“下一步”按钮,稍候完成制作 DOS 启动盘的任务。

(3) DOS 下运行 Norton Ghost 2001 制作磁盘分区的整体备份(映像文件)

① 使用上面制作的可以在 DOS 下引导的 Ghost 启动盘重新启动,并引导计算机。

② 在 DOS 下启动之后,将自动运行 Norton Ghost 2001 程序,激活如图 14-5 所示的窗口。如果不能自动启动鼠标,可以先运行软盘中的 Mouse.exe 程序,再运行



图 14-4　创建“Norton Ghost 引导盘”的目标驱动器窗口

“A:\Ghost\Ghostpe.exe”程序，也可以激活如图 14-5 所示的窗口。

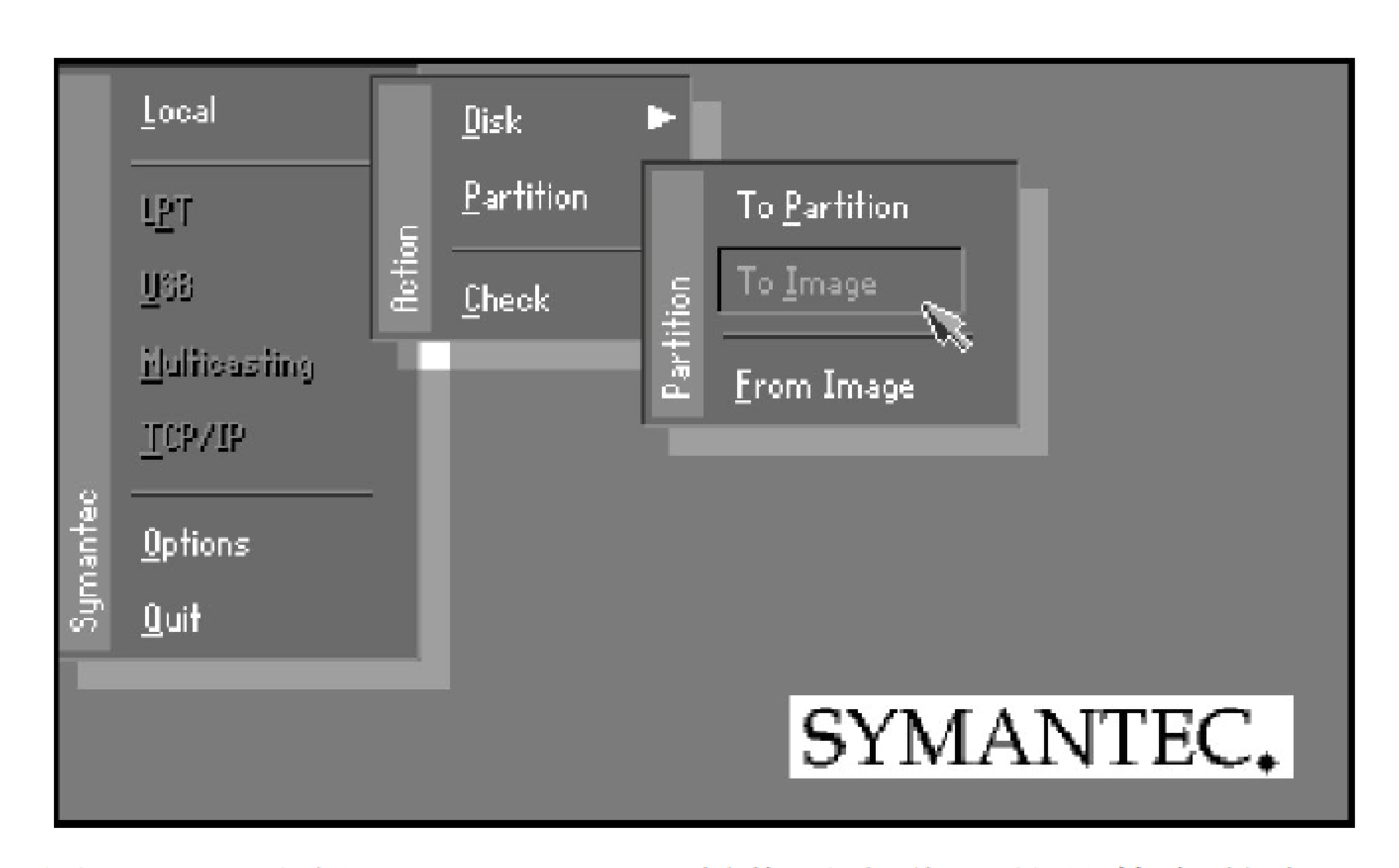


图 14-5　选择 Norton Ghost 制作磁盘分区的整体备份窗口

③ 在图 14-5 所示的窗口中，依次选择 Local→Partition→To Image 命令选项，激活如图 14-6 所示的窗口。

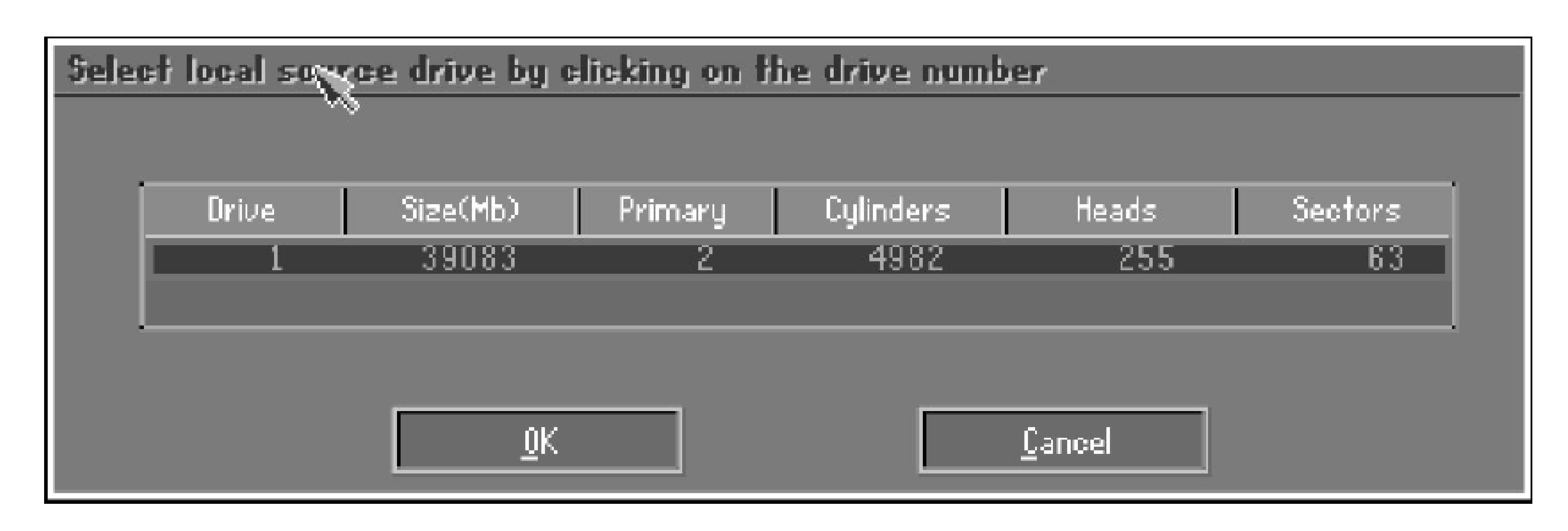


图 14-6　使用 Norton Ghost 进行磁盘分区整体备份的“源驱动器选择”窗口

④ 在图 14-6 所示的窗口中，单击 OK 按钮，激活如图 14-7 所示的窗口。

⑤ 在图 14-7 所示的窗口中，选择并单击所要备份的分区，然后单击 OK 按钮，激活后继的窗口。

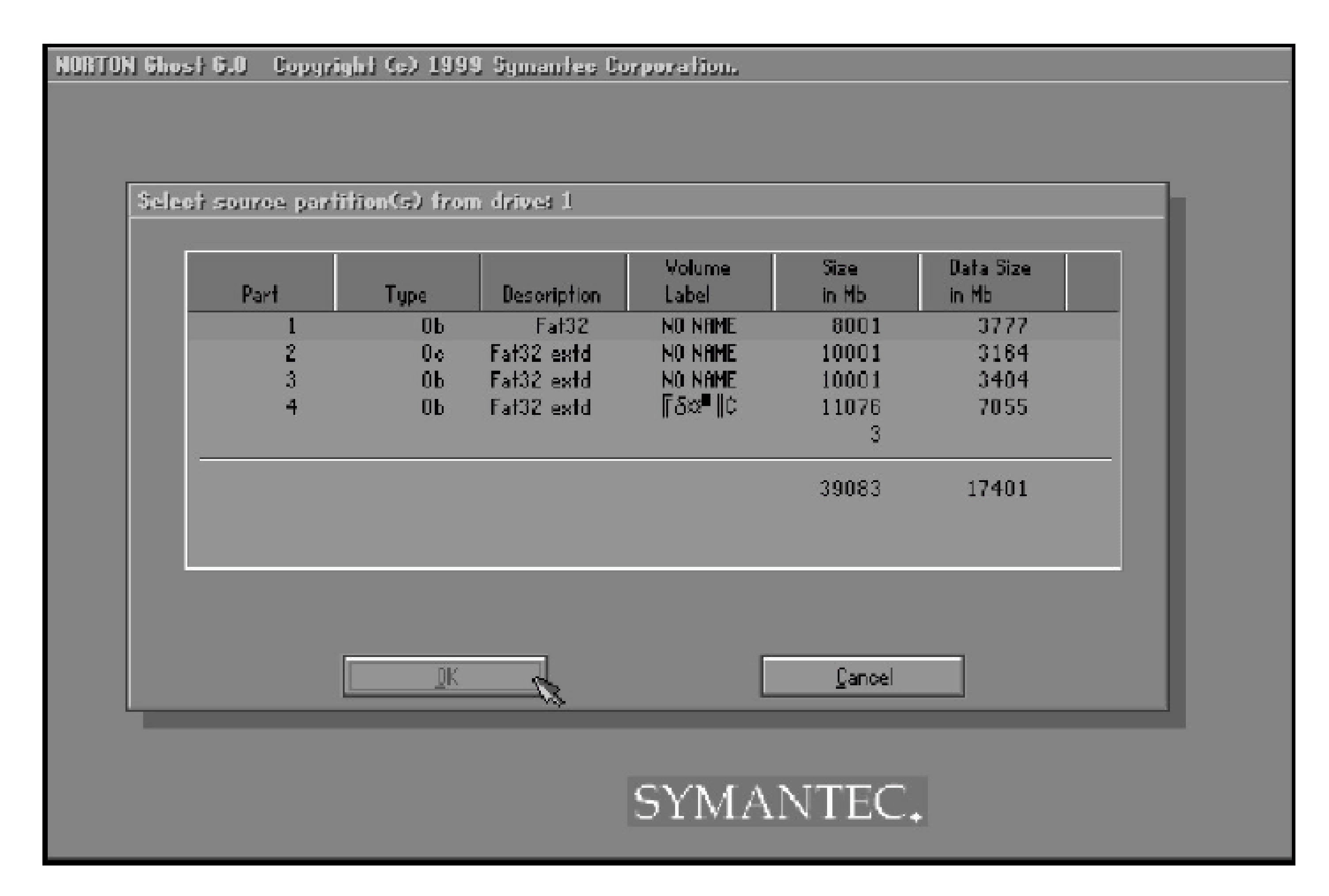


图 14-7　使用 Norton Ghost 进行磁盘分区整体备份的“源分区选择”窗口

⑥ 在激活的下一个窗口中，需要对选定的硬盘、分区等进行仔细的核对，确认之后，输入一个整体备份文件的名字，例如 WINNT ServerBAK，然后按 Enter 键继续。

⑦ 在后继的窗口中，屏幕会提示 3 个选择项，分别是 NO，FAST 和 HIGH。

- NO　备份时不进行压缩处理，所以体积大，但速度最快。
- FAST　备份中进行一定的压缩处理，体积中等，速度比较快。
- HIGH　备份时压缩，压缩后体积小，但进行速度较慢。

用户可以根据自身的需要进行选择，之后单击“确认”，即可开始 Ghost 的备份工作。

3. 引导分区整体备份的恢复

当所备份的引导分区出现致命错误时，可以不必重新安装该分区上的系统和所有应用程序，只需再次运行上述的 Ghost.exe 程序，依次选择 Local→Partition→From Image 命令选项，并选定原先整体备份文件的存放位置，即可恢复原来分区中的所有内容。

使用所备份的映像（也叫镜像）文件恢复引导分区整体备份的步骤如下：

① 使用前面制作的 Ghost 引导盘（A 盘）重新启动，并引导计算机。

② 在 DOS 下启动之后，将自动运行“Norton Ghost 2001”，激活如图 14-4 所示的窗口。如果不能自动启动，先运行软盘中的 Mouse.exe 程序，再运行“A:\Ghost\Ghostpe.exe”程序，也可激活如图 14-4 所示的窗口。

③ 在图 14-4 所示的窗口中，依次选择 Local→Partition→From Image 命令选项。

④ 选定整体备份文件，即扩展名为“.gho”的映像文件。

⑤ 指定映像文件所要恢复的分区，例如：通常为用户计算机磁盘的第一个主分区。选定并确认后，Ghost 即可开始自动进行该分区映像文件的恢复工作。

注意：*第一，Ghost 映像文件的扩展名为“.gho”；第二，请一定要仔细选择和核对所选的映像文件是否与你要恢复的分区相符，否则，不能正确恢复分区；第三，在一般的 PⅡ 计算机上，1GB 的硬盘映像文件的恢复时间约为 10 分钟左右。*

4. 使用“Ghost 浏览器”制作备份文件

安装 Norton Ghost 2001 程序之后，该程序组中的另一个有用工具就是“Ghost 浏

览器”。

（1）“Ghost 浏览器”的功能

① 查看映像文件的内容，并保存映像文件内的文件列表。

② 从映像文件还原文件或目录。

③ 在所选择的映像文件内，可以随时添加、移动、复制、删除和启动文件。

④ 可以使用拖放、剪切、粘贴等功能从 Windows 的资源管理器中向映像文件添加文件或目录。

（2）使用“Ghost 浏览器”和“资源管理器”制作备份文件

“Ghost 浏览器”窗口的使用方法与“Windows 资源管理器”的使用方法十分相似。例如：可以在 Norton 的“Ghost 浏览器”窗口内，选定一个文件或目录并单击鼠标右键，从弹出的文件的快捷命令列表中进行选择。如果用户需要帮助信息，请在 Norton“Ghost 浏览器”中单击“帮助”菜单命令。

① 依次选择“开始”→“程序”→“Norton Ghost 2001”→“Ghost 浏览器”命令选项，激活如图 14-7 所示的“Ghost 浏览器”窗口。

② 选择“开始”→“程序”→“Windows 资源管理器”命令选项。

③ 在激活的“Windows 资源管理器”窗口中，选择需要归档的目录或文件后，使用鼠标可以将其直接“拖拽”到“Ghost 浏览器”的窗口中。例如：在“资源管理器”窗口中选择了“刻录盘”目录后，按住鼠标左键，将所选目录“拖拽”到“Ghost 浏览器”的窗口，完成归档备份的任务。

④ 如果所选的归档文件已经存在，将激活如图 14-8 所示的“确认文件替换”窗口，用户可以根据自身的需要进行选择。



图 14-8 “Ghost 浏览器”窗口

5. Norton Ghost 2001 的其他数据保护功能

除了上述功能外，Norton Ghost 2001 还可以完成以下几种功能。要完成这些功能，首先必须将两块或多块硬盘安装在同一机器上，也可以先使用 hub（集线器）和网卡分别连接两台或多台计算机，然后，使用制作好的 DOS“对等网启动软盘”分别启动两台计算

机上的 Ghost.exe 系统。

(1) 硬盘间的复制

网络中通常配备有两个或多个相同容量的硬盘,网络管理员可以先为其中一个硬盘安装并配置好可以正常运行的操作系统及应用程序,对于其他多个空白的硬盘,则无须重复安装同样的操作系统和应用程序,利用 Norton Ghost 2001 程序,可以在很短的时间内将第一个硬盘中的内容原样复制到其他硬盘中。例如:第一个硬盘安装好 WIN 98/NT 以及 Office 2000 之后,使用 Ghost 在很短的时间内就可以完成其他多个硬盘的安装、配置工作。其主要步骤简述如下:

① 先将两个硬盘安装在同一台计算机中,或者使用制作好的 DOS“对等网的启动软盘”,分别从 DOS 下启动两台已联网的计算机。注意,Ghost 程序虽然有时也能在 WIN 98 下运行,但为了防止意外情况发生,还是推荐用户在 DOS 环境下运行 Ghost.exe 程序。

② 在 DOS 下启动之后,将自动运行 Norton Ghost 2001,激活如图 14-5 所示的窗口。如果不能自动启动鼠标,请先运行软盘中的 Mouse.exe 程序,再运行 A:\Ghost\Ghostpe.exe 程序,可以激活如图 14-5 所示的窗口。

③ 在图 14-5 所示的窗口中,依次选择 Local→Disk→To Disk 命令选项。

④ 在 DOS 状态下运行上述命令之后,在激活的窗口中,应选择和设置好硬盘的主/从状态。Ghost 会显示出两个磁盘的详细情况。

⑤ 先选择第 1 个硬盘(源盘),并按照 Ghost 的提示进行确认。

⑥ 再选择第 2 个硬盘(目标盘),进行确认之后,Ghost 就会开始“盘对盘”的复制工作。

⑦ 屏幕上将有蓝色的进度条,显示其进行的状态。一般地,1GB 左右的数据硬盘,在 10 分钟左右就可以完成复制工作。

注意:

- 在选择“源盘”和“目标盘”时,请千万仔细核对,不要弄错。如果选择反了,复制完成之后,就只剩下两个空白硬盘了。
- 对于不同容量的两个硬盘,使用此方法,只能从容量小的硬盘复制到容量大的硬盘上;反之,则不行,因为 Ghost 会将复制后的硬盘的剩余空间做了空闲处理,所以,用户只能通过分区软件,将剩余的空间找出。
- 对于具有坏道的硬盘来说,进行上述复制操作后,系统运行会变得不稳定。

(2) 从硬盘到映像(镜像)文件

如果用户的服务器上有多个硬盘,就可以使用其他硬盘来备份正在使用中硬盘内的数据。

① 先将两个硬盘安装在同一台计算机中,或者使用制作好的 DOS“对等网的启动软盘”分别从 DOS 下启动两台已联网的计算机。

② 在 DOS 下启动之后,自动运行 Norton Ghost 2001,激活如图 14-5 所示的窗口。

③ 在图 14-5 所示的窗口中,依次选择 Local→Disk→To Image 命令选项。

④ 在 DOS 状态下运行上述命令之后，在激活的窗口中，应选择和设置好硬盘的主/从状态。Ghost 会显示出两个硬盘的详细情况。

⑤ 接下来，首先选定要备份的硬盘，再选定映像(镜像)文件的存放位置。例如，通常先在第二个硬盘中建好一个目录，然后，指定该目录为映像文件的存放位置。

⑥ 随后，在屏幕下端的提示栏中，输入拟生成的映像文件的名字，例如"DISK_IMG"。

⑦ 按 Enter 键后，即可开始进行与前面分区备份类似的工作了，界面窗口中同样会有一个进度条，演示进度的进行过程。

(3) 从映像(镜像)文件恢复硬盘内容

经过以上的备份之后，当硬盘损坏时，即可使用所制作的硬盘备份文件，恢复硬盘中原有的内容。

① 先将两个硬盘安装在同一台计算机中，或者使用制作好的 DOS"对等网的启动软盘"分别从 DOS 下启动两台已联网的计算机。

② 在 DOS 下启动之后，自动运行 Norton Ghost 2001，激活如图 14-5 所示的窗口。

③ 在图 14-5 所示的窗口中，依次选择 Local→Disk→From Image 命令选项。

④ 在打开的窗口中，选择先前所备份的映像文件的存放位置和名称，例如"DISK_IMG"。

⑤ 接下来，指定要恢复到哪一个硬盘。确认之后，Ghostpe.exe 恢复工具就开始恢复系统。

(4) 从分区到分区的复制

用户有时会有这样的要求，即在两个不同硬盘的某个分区上，打算安装相同的操作系统和工具软件，但两个硬盘的其他分区可能不同，使用 Ghost 可以方便地完成这样的工作。

在 Norton Ghost 2001 程序的窗口中选定相应的分区之后，Ghost 即可开始工作，进度条可以展示进度的进程。完成之后，就有两块启动分区相同，而其他分区内容不同的硬盘了。

注意： 由于是分区对分区的复制，因此，要求两个硬盘中所要进行复制的分区的大小必须一致，如果不一致，目标盘的其他分区将被删除。

(5) 将分区复制到映像(镜像)文件

将分区内容复制到映像(镜像)文件的功能是用户最常使用的功能，也就是前面所介绍的分区整体备份的操作。例如，使用此功能，可以备份装有 WIN 98 操作系统，及其所有硬件驱动程序和应用程序的客户机的主分区内容，也可以备份用户打算备份的其他分区中的所有内容。

当前，由于计算机的硬盘都比较大，通常会划分有多个分区，习惯上 C 盘上安装有 WIN 98 系统和一些常用的工具。因此，做 C 盘(即主引导分区)的整体备份(包括其中的操作系统、驱动程序和全部应用程序)的意义是不言而喻的。完成此功能，无需使用第二个硬盘，只需将映像文件存放在其他分区中即可。

① 在 DOS 下启动并执行 Ghost.exe 后，出现图 14-5 所示的 Ghost 主界面窗口，依次选择 Local→Partition→To Image 命令选项。

② 在随后激活的窗口中，选定硬盘和分区。

③ 确认之后，选择并输入映像（镜像）文件所在位置及其名称，例如，存放在 E 盘，名称为 WIN_98BAK，然后按 Enter 键。

④ 屏幕会提示 3 个选择项，分别是 NO，FAST 和 HIGH。这 3 个选项的含义前面已经介绍了，用户可以根据自身的需要进行选择。

⑤ 用户确认后，Ghost 开始进行备份工作。

（6）检查功能

Ghost 的检查功能可以用来检查映像文件及磁盘的工作状态是否良好，该功能的应用不太广泛。

（7）LPT 传输功能

Ghost 的 LPT 传输功能支持计算机的 LPT（并口）数据传输功能。例如，用户可以通过 LPT（并口）线连接笔记本电脑和台式计算机，并进行数据交换。

6. 使用 Winrar.exe 进行归档备份和增量备份

对于用户指定的数据文件可以选择使用 WinZip.exe 和 Winrar.exe 进行各种备份，例如归档或增量备份等。

14.3 Windows NT 中的备份程序

Windows NT 中完成数据保护功能的一个程序就是备份程序。

1. Windows NT 备份程序的作用

Windows NT 备份程序是保护数据免遭意外丢失或硬件和介质错误的工具。利用备份程序可以方便地使用磁带机在 Windows NT 文件系统（NTFS）或文件分配表（FAT）文件系统上“备份”或“还原”重要文件。

2. Windows NT 备份程序的功能

在计算机应用系统中，磁盘的数据是非常重要的，在 Windows NT 中，将磁盘数据复制到磁带机上的工具名称为“备份”（backup），它是 Windows NT 中从磁盘到磁带存储的简单程序，其功能和操作特点如下：

① 使用计算机上附带的磁带机，“备份”或“还原”NTFS 或 FAT 卷上的本地或远程文件。

② 要备份或还原的文件，能够以卷、目录或单个文件名的方式选定，还可以查看文件详细信息。例如备份文件的大小及更改日期等。

③ 应确定以校验方式传送，以确保“备份”或“还原”的可靠性。

④ 能够实现任一通用备份的操作，例如，实现“普通（整体）”、“复制（归档）”、“增量”、“差量”和“日常复制”备份等的“备份”或“还原”操作。

⑤ 在磁带上放置多个备份集、添加新备份集或者用新的备份集覆盖整个磁带。因为

没有文件大小的限制,所以备份集和文件可以包括多个磁带。

⑥ 可以创建批处理文件,实现自动、重复备份驱动器。

⑦ 可以查看备份集的全部目录、单个文件以及目录的信息,以选定要还原的文件。

⑧ 当还原操作要覆盖最近创建的文件时,能够控制还原操作的目标驱动器和目录,并接受可采取操作的适当选项。

⑨ 将磁带操作的日志信息保存到文件,并且在 Windows NT "事件查看器"中查看磁带操作信息。

综上所述,NT 备份程序具有如下 3 个最主要的功能特点:

- 备份(backup)程序的主要功能　在 Windows NT 所支持的文件系统上"备份"或"还原"重要的数据和程序文件。
- 备份时有多种灵活的操作选择　例如,数据操作的对象可以是卷、文件夹和单个文件。
- 能够以自动方式或手动方式进行操作　自动方式通过创建批处理文件的方式得以实现;手动方式操作可以查看磁带上备份集数据文件的详细信息来确定需要还原的文件。

说明: 受篇幅所限,本书就不再介绍 Windows NT 中的备份程序的使用。

14.4　数据容错技术

容错技术是数据保护系统使用的另一种技术。

1. 容错和容错技术

容错是系统的一种容忍故障的能力。容错技术的使用使得系统在局部(软件或硬件)损坏后,仍能完成数据的处理和运算。系统因使用了容错技术而具有继续工作的能力。一般,容错技术通过冗余资源使得系统具有这种容忍故障的能力。

2. 容错技术解决和处理的常见问题

容错技术解决和处理的常见问题如下:

① 引导文件的损坏。

② 操作系统本身,或者是操作系统文件的损坏。

③ 由磁盘损坏、电源掉电,或者是操作系统中断等引起的问题。

3. RAID 数据冗余

(1) RAID 数据冗余的基本概念

RAID 通过数据冗余(data redundancy)来提供容错。数据冗余是指将相同的数据同时写入多个硬盘,这样当其中一个硬盘被损坏后,数据仍可恢复。

RAID 技术是标准化的,并且按级别进行分类。每个级别的性能、可靠性和所需要的费用都是不同的。

(2) RAID 容错系统的选择

RAID 容错系统可以通过软件和硬件来实现。到底是选择通过硬件实现,还是通过

软件来实现不能一概而论，但都应当注意以下几个问题：

① 软件容错比硬件容错便宜。

② 软件容错比硬件容错系统的速度慢。

③ 硬件容错的解决可能过分依赖于某个硬件销售商。

④ 在硬件容错系统中，某些服务商能够提供“在线”（即不关机）更换被损坏的驱动器的服务功能。

4. Windows NT 服务器支持的 RAID 数据冗余技术

Windows NT 服务器支持两种基于 RAID 数据冗余的容错技术：镜像集（RAID 1）和带奇偶检验的带区集（RAID 5）。

（1）RAID 1——镜像集（mirror set）

镜像集（RAID 1）工作的原理如图 14-9 所示。RAID 1 系统使用 Windows NT 容错驱动程序 ftdisk.sys 将同一个数据同时写入两个物理的硬盘驱动器，这种方式称为“双重写入”或者是“镜像”技术。

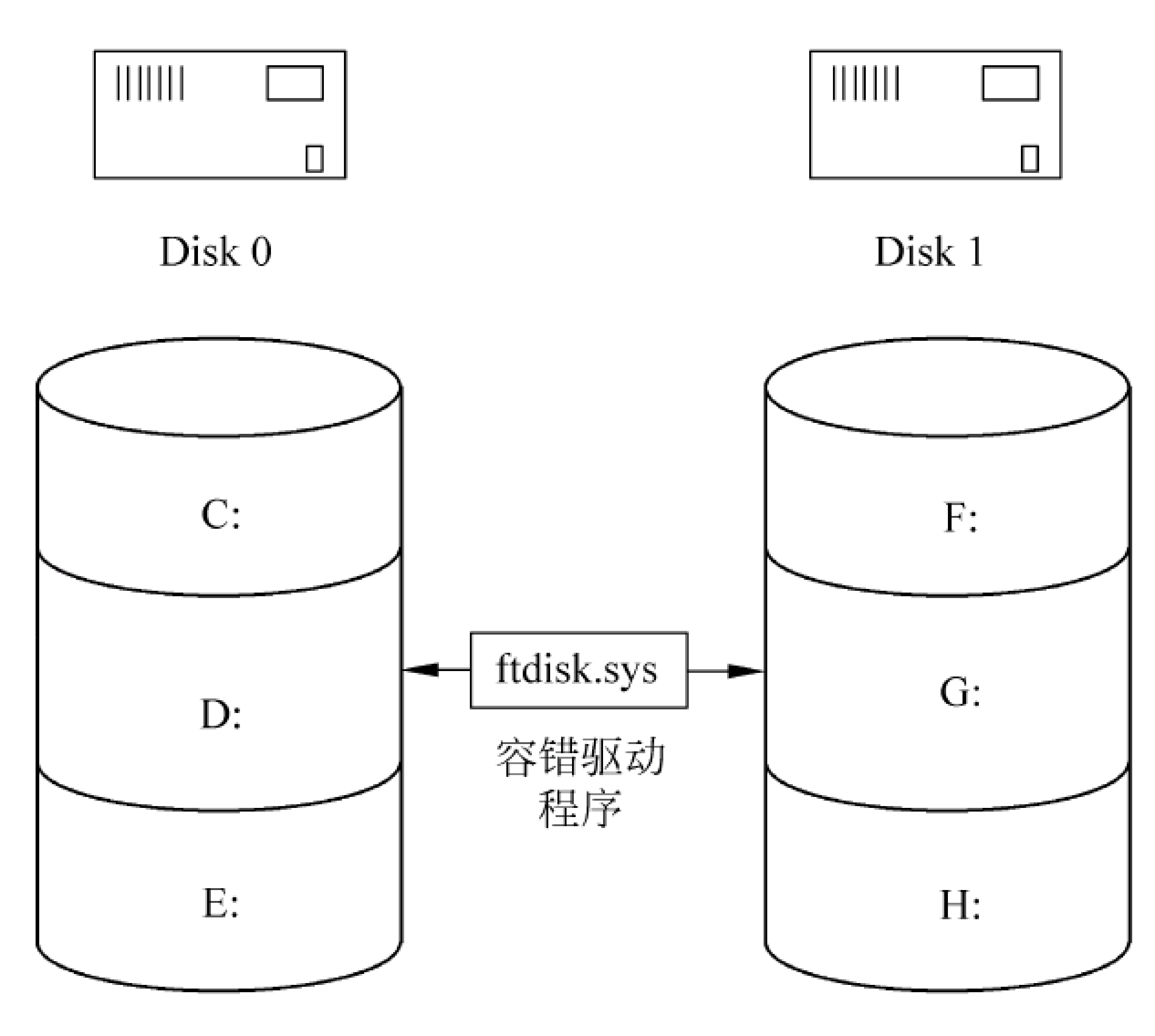


图 14-9　磁盘镜像——RAID 1

如果需要使系统分区或引导分区具有容错能力，目前，最好采用 RAID 1“镜像集”方式。采用此方式最利于系统崩溃后的迅速恢复。

镜像集（RAID 1）利用将一个分区的数据重复写入到另一个物理硬盘的方法来对付系统崩溃。其原理如图 14-9 所示，在磁盘 disk0 驱动器 D 上的数据被重复写入到 disk1 的驱动器 G 中。由于引导或系统分区均可以生成镜像，因此，Windows NT Server 是在逻辑字母驱动器上设置容错，而不是在物理磁盘级上设置容错。

（2）RAID 5——带奇偶检验的带区集（stripe set with parity）

奇偶检验是验证数据完整性的数学方法。“带奇偶检验的带区集”通过向卷中的每一个磁盘分区增加一个检验信息来实现容错功能。RAID 5“带奇偶检验的带区集”将未格式化的自由空间组合成一个大的逻辑驱动器，并在保存的数据中增加了奇偶检验数据，当某个硬盘发生故障而无法读取时（例如：硬盘中的电源中断），即可利用此奇偶检验数据

推算出故障硬盘中的数据。

Windows NT 的“带奇偶检验的带区集”利用将要写入的所有硬盘数据,先做 XOR (Exclusive OR)即“异或”逻辑运算操作,并将该操作中所得的结果作为奇偶检验数据。这个数据并非保存在固定的硬盘中,而是按照顺序分布在每个硬盘中,例如:第 1 次保存到驱动器 0(disk 0)、第 2 次保存到驱动器 1(disk 1)、……依次类推,直到保存到最后一个硬盘后,再从驱动器 0 开始保存。在实现“带奇偶检验的带区集”时至少需用 3 个硬磁盘。

“带奇偶检验的带区集”具有非常高的读取速率,这是因为读取数据时,是同时由多个硬盘中读取;写入时,虽然在计算奇偶检验数据时浪费了一些时间,但是整体效率还是非常高的。

在 Windows NT 的带区集中,将数据平均写入所有的硬盘中,以每次写入一行的方式,64KB 为单位来进行写操作。它对带区集的所有硬盘执行同一功能,执行时很像是单个硬盘的操作。带区集提供了同时发出 I/O 命令,并在所有硬盘上同时处理它们的功能。因此,带区集可以提高系统的 I/O 速度。

带奇偶检验的带区集可以支持 3～32 个磁盘,利用这种技术可以重建因物理磁块损坏而需要重建的数据。如果发生单一磁盘的损坏,数据不会丢失,这是因为 Windows NT Server 的容错程序,已经将同一信息散开到其余的磁盘上了,所以数据能够被完整地重建出来。

5. 在 Windows NT Server 中实现容错的工具

在 Windows NT Server 中实现容错的工具是磁盘管理器,其主要功能如下:

(1) 创建和删除硬盘上的分区和扩展分区中的逻辑驱动器

① 格式化及生成卷标。

② 读取磁盘的状态信息。例如,读取某分区的大小,检查可用来创建其他分区的剩余空间的尺寸。

③ 读取 Windows NT 卷的状态信息。例如指定的驱动器号、卷标、文件系统类型与大小。

④ 指定并更改分配给硬盘卷和 CD-ROM 的驱动器号等。

⑤ 创建并删除卷集。

⑥ 扩展卷和卷集。

⑦ 创建并删除带或不带奇偶检验的带区集。

(2) 再生带奇偶检验的带区集的丢失或失效部分,以及创建或取消磁盘镜像集

6. Windows NT Server 中容错工具“磁盘管理器”的使用

在系统软件 NT Server 的安装过程中,就可以对计算机的硬盘分区进行选择和设计。系统安装之后,用户可以利用“磁盘管理器”更改已安装系统的磁盘分区,还可以利用它对新安装的附加硬盘进行分区。但是,“磁盘管理器”不能够对安装了 NT 系统的分区再进行分区操作,因为该分区中含有 Windows NT Server 所需的文件。

启动和使用磁盘管理器的步骤如下:

① 以 administrator 组成员的身份登录。只有系统管理员组的成员才具有打开“磁盘管理器”的权限。

② 依次选择“开始”→“程序”→“管理工具”→“磁盘管理器”命令选项。

③ 首次进入时，将激活“磁盘管理器”程序提示窗口，单击“确定”按钮，激活如图14-10所示的窗口。

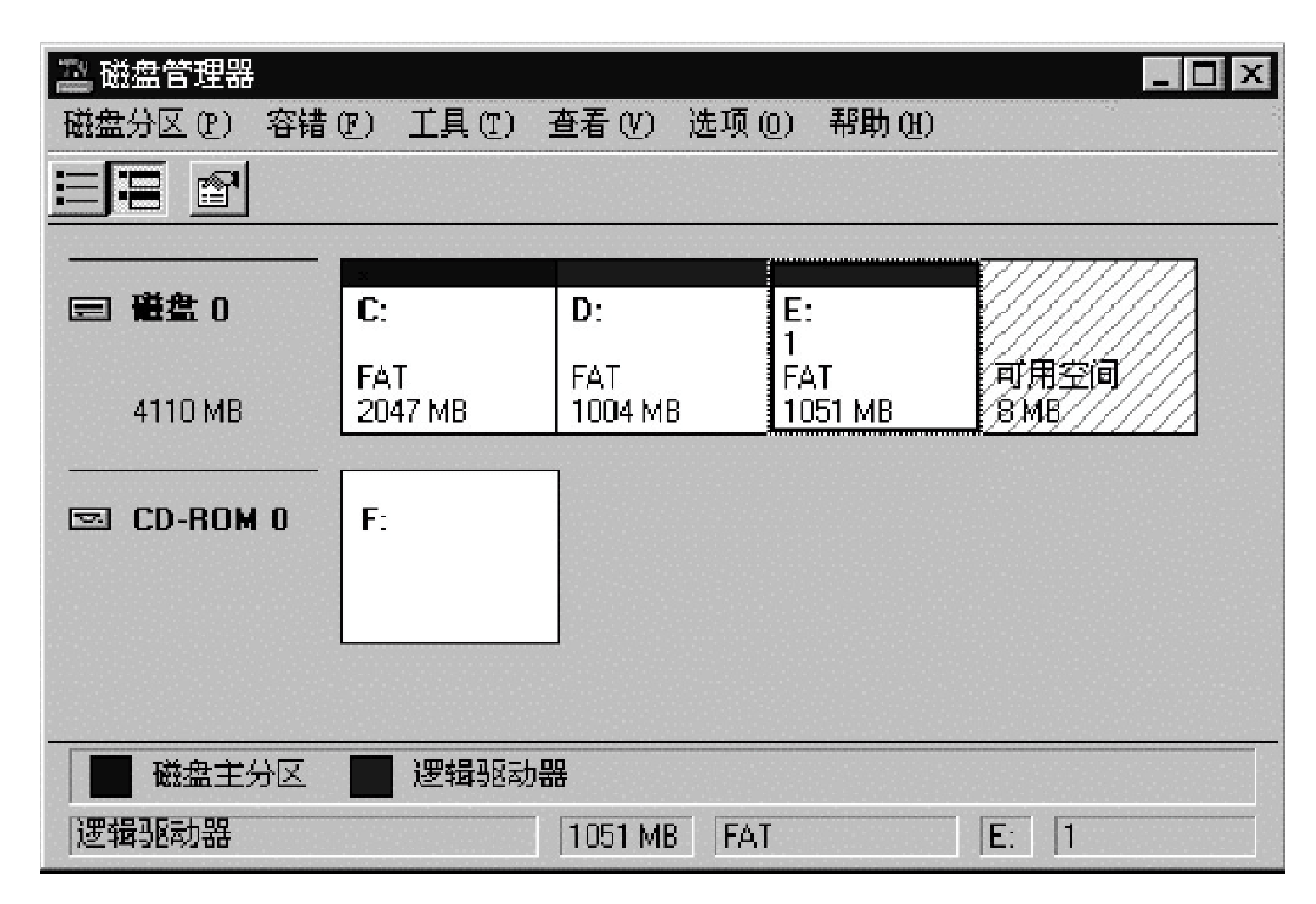


图 14-10 “磁盘管理器”工作窗口

④ 在图14-10所示的“磁盘管理器”工作窗口中，单击“帮助”命令，可以激活“帮助主题：磁盘管理器帮助”窗口，单击其中的“目录”选项卡，可以选择需要查询的帮助主题。

说明：由于篇幅所限，本节不再详细介绍如何使用“磁盘管理器”程序。

14.5 Windows NT 中的其他数据保护方法

形象地说，网络管理员就是网络的“值班医生”，网络中的所有计算机就是网络管理员的“病人”，那么如何迅速地对症下药，就是每个网络管理员应逐步掌握的基本技能。

系统管理员的主要职责是维护、管理计算机网络，在管理网络时还有一项重要任务就是系统数据的恢复，当网络系统被损坏，不能正常启动时，网络管理员应当能为网络用户提供快速、准确的服务，及时地修复或恢复被损坏的系统数据，使用户能够尽快地正常使用计算机网络中的所有资源和服务。

尽管整体备份使得网络管理员可以在最坏的情况下恢复Windows NT系统，但其恢复的速度较慢，方法也比较复杂。因此，在NT网络中，除了标准的备份与容错方法外，还有其他一些系统和数据的保护方法。

对于日常性的维护工作，采用“备份”的方法有时并非完全合适，因为，当系统数据被损坏时，使用“备份”的方法，需要先格式化硬盘，再重新恢复系统数据。而日常工作中出现的大多数问题，可能只是注册表(registry)损坏、引导文件被破坏等小问题，在这种情况下，用户就大可不必采用“备份”的复原技术，而可以先采用本节所推荐的其他数据保护方法进行系统的快速修复。如果修复失败，再使用整体硬盘或部分分区备份恢复的方法复原系统数据。

当不明原因导致NT系统无法正常启动时，应该选择哪种方法恢复系统数据，并使其

恢复正常的功能呢？严格讲，由于NT系统很大，因此无论采用哪种方法来修复系统都不会尽善尽美，所以任何方法都不是万能的。下面，将介绍几种常用的、行之有效的较快速的修复或恢复NT系统的方法，用户可酌情选用。

14.5.1 利用“上一次的正确系统配置”恢复NT系统

当用户由于以下原因而无法正常启动NT系统时，可以尝试利用“上一次的正确系统配置”的环境启动系统。

1. 利用“上一次的正确系统配置”恢复NT系统的适用场合

这种恢复方法适用于以下场合：

① 新增驱动程序后无法正常启动NT系统。

② 用户修改了Registry数据库后无法正常启动NT系统。

2. 利用“上一次的正确系统配置”恢复NT系统的步骤

这种方式的实质是还原注册表，其操作步骤如下：

① 当系统故障时，首先选择“开始”，然后单击“关闭系统”。

② 选择“重新启动计算机”，然后单击“是”按钮。

③ 在提示下，按空格键启动“硬件配置文件/已知的最新正确配置”菜单，该菜单将注册表还原到稳定状态。

④ 按照屏幕上的指示操作。

注意：按照上述过程，可以将注册表还原为上次成功启动时的状态。

说明：本节所介绍的方法虽然恢复时间短，但是不适合因为驱动程序或文件损坏、丢失所造成的不能启动的状况。遇到这种情况时，可以尝试采用本节所介绍的其他方法修复被损坏的NT系统。

14.5.2 利用“紧急修复磁盘”修复被损坏的NT系统

无论是安装了NT Server的服务器，还是安装了NT Workstation的客户工作站，均可以使用下述方法恢复被损坏的NT系统。当NT的系统文件、启动变量或启动分区被损坏，而且无法利用“上一次的正确系统配置”的环境启动时，请利用“紧急修复盘”和3张系统引导“安装磁盘组”恢复被损坏的NT系统。该方法恢复系统时，操作简单，恢复时间中等。

1. 紧急修复盘的制作

在安装NT的工作站或服务器时，都会提示用户制作一张“紧急修复磁盘”，这张磁盘中包含了修复系统所必需的数据。对系统管理员来说，应该及时制作“紧急修复盘”，并且必须定期更新这个磁盘。制作与更新“紧急修复磁盘”的步骤如下：

① 依次选择“开始”→“运行”命令选项，激活“运行”窗口。

② 在“运行”窗口中，在“打开(O)：”文本框内，键入程序名称rdisk，单击“确定”按钮，激活图14-11所示的“磁盘紧急修复实用程序”窗口。

③ 在图14-11所示的窗口中，可以根据需要进行选择，例如，单击“更新修复信息”按

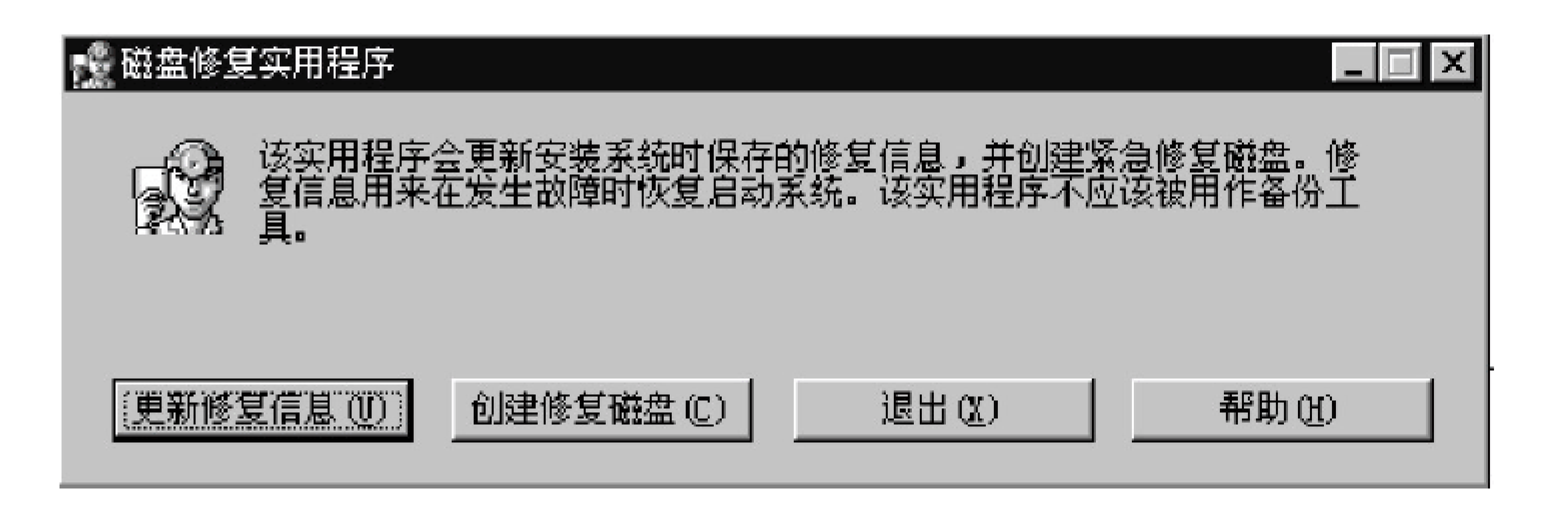


图 14-11 “磁盘紧急修复实用程序”窗口

钮，或单击“创建紧急修复磁盘”按钮。之后，可以根据屏幕提示完成此项工作。

2. 利用3张系统引导“安装磁盘组”和“紧急修复磁盘”恢复NT系统

① 如果在安装NT系统时，没有制作三张“安装磁盘组”，或“安装磁盘组”中的某些磁盘已损坏时，可以在DOS下，转入“\I386目录(NT工作站或服务器)”，运行命令“winnt /ox”，补充制作setup boot disk、setup disk 2和setup disk 3这三张用于引导NT安装系统的“安装磁盘组”。

② 将Windows NT工作站或服务器4.0中文版光盘放入CD-ROM。

③ 将setup boot disk磁盘放入软盘驱动器，引导系统，当出现“欢迎使用安装程序”的信息时，可以有图14-12所示的4种选择，请选择“修复上次安装时损坏的4.0中文版Windows NT”选项，即键入R。

在安装前如果想多了解Windows NT的安装过程，请按F1。
开始安装Windows NT，请按ENTER。
修复上次安装时损坏的4.0中文版Windows NT，请按R。
停止安装Windows NT，并退出安装程序，请按F3。

图 14-12 Windows NT安装程序安装选项

④ 跟随NT安装磁盘的向导，分别插入“安装磁盘组”中的各个磁盘和“紧急修复磁盘”，即可完成NT系统的恢复工作。

3. 恢复的内容和注意事项

① 使用制作“紧急修复磁盘”时的“用户账号”和“密码”注册新恢复的系统。

② 恢复时需要3张引导系统的“安装磁盘组”、1张“紧急修复磁盘”和用于安装的原版Windows NT Server 4.0的CD-ROM盘，或者是在硬盘中复制的Windows NT Server 4.0盘中的I386目录。

③ 3张引导系统的“安装磁盘组”的磁盘被损坏时的制作方法如下：

- 使用“winnt /ox”(DOS命令)制作3张引导系统的“安装磁盘组”。
- 在Windows NT下，运行命令rdisk可以制作“紧急修复磁盘”。

④ 在前面已经介绍了恢复系统的方法及步骤，所恢复的内容如下所述：

- Autoexec.nt　这是%Systemroot%\System32\Autoexec.nt文件的副本，用来启动MS-DOS的环境。
- Config.nt　这是%Systemroot%\System32\Config.nt文件的副本，用来启动MS-DOS的环境。

- Default._　这是 HKEY_USERS\DEFAULT 的内容，为压缩文件。
- Ntuser.DA_　这是%Systemroot%\Profiles\DefaultUser\Ntuser.dat 文件的副本，为压缩文件。硬盘上的 Ntuser.dat 文件损坏时可用此文件恢复有关数据。
- Sam._　这是 HKEY_LOCAL_MACHINE\SAM 的内容，为压缩文件。
- Security._　这是 HKEY_LOCAL_MACHINE\SECURITY 的内容，为压缩文件。
- Setup.log　这记录已安装文件与 CRC(cyclic redundancy check)的有关数据，以供修复时使用。它的文件类型为只读、系统和隐含，用户可以在“Windows NT 资源管理器”或“我的电脑”中，选择“查看”→“选项”命令，然后单击“查看”选项卡，选中“查看所有文件”的属性后，就能看到此文件。
- Software_　这是 HKEY_LOCAL_MACHINE\SOFTWARE 的内容，为压缩文件。
- System　这是 HKEY_LOCAL_MACHINE\SYSTEM 的内容，为压缩文件。

上述各文件是带有“下划线”的压缩文件，若需要单独恢复，可使用硬盘 NT 目录下的解压程序先行解压，例如，使用“winnt\SYSTEM32\expand.exe”程序对欲解压的文件进行解压后，再将解压程序复制到原来的位置。

14.5.3　利用“注册表”修复被损坏的 NT 系统

1. 注册表(registry)概述

(1) 注册表及其重要性

系统注册表是一组存储系统软件、硬件、应用程序和用户信息的文件集合。注册表的设计目的是为了替代以前保留此类信息的系统配置文件，例如，在 MS-DOS 中的 config.sys 和 autoexec.bat；在 Windows 早期版本中的 win.ini 和 system.ini 等文件。

注册表的内容是非常重要的，它是 NT 系统的核心。例如，当黑客可以自由访问注册表的时候，他们就可以访问整个系统了。如果注册表被破坏，只有重装系统才能恢复。当然，也可以使用系统正常时的备份重新恢复系统。

注意： 由于注册表是保存系统配置等重要数据的数据库，因此，请不要随意修改注册表的值，以避免系统无法正常运行。

(2) 注册表的功能和内容

在 NT 中运行 regedt32.exe 和 regedit.exe 程序，可以查看或修改有关注册表的信息。其中 REGISTRY 为注册表，它包含了注册表数据库的全部内容，包括计算机的默认设置和用户的一些特殊的设置，例如，自定义的启动画面、不需要登录即可关闭系统、自动登录等设置。

① 注册表“HKEY_LOCAL_MACHINE”　这里保存了本计算机系统中的所有配置信息，包含硬件的设备驱动程序、应用程序和 NT 操作系统的使用以及本地计算机的配置数据，例如，系统内存、驱动程序、安全数据库和系统配置等信息。

② 注册表“HKEY_CLASS_ROOT”　保存与关联(association)有关的信息。它也

包括与COM(component object model)有关的OLE信息。此处包含的数据与HKEY_LOCAL_MACHINE\Software\Classes中的信息相同。

③ 注册表"HKEY_CURRENT_CONFIG" 保存与硬件配置文件(hardware profile)有关的数据。

④ 注册表"HKEY_USERS" 保存当用户登录时,所有必须载入的用户配置文件数据,包含默认的配置文件(default profiles)和登录者的环境配置文件(HKEY_CURRENT_USERS)。其中,保存了两个主要关键字,一个是DEFAULT,它包含了当显示"CTRL+ALT+DEL"登录屏幕时,使用的系统默认设置信息;另一个是ID,它包含了当前登录用户的安全ID等信息。

⑤ 注册表"HKEY_CURRENT_USERS" 保存与当前登录用户(current user)有关的环境设置数据,例如桌面和网络连接以及当前交互式登录到计算机上的用户信息。

要进一步了解注册表的功能,请参阅readme.wri文件。

2. 使用注册表修复被损坏的NT系统

(1)"注册表编辑器"的启动

如果用户是NT系统的高手,希望自行定义注册表的环境参数,那么,首先需要运行注册表程序,激活"注册表编辑器"。

"注册表编辑器"是用于更改系统注册表设置的高级环境工具。启动"注册表编辑器",需要运行regedit和regedt32程序,其步骤如下:

① 依次选择"开始"→"运行"命令选项,激活"运行"窗口。在窗口的"打开(O):"文本框内,键入程序的路径和名称regedit.exe,然后,单击"确定"按钮,激活如图14-13所示的窗口。

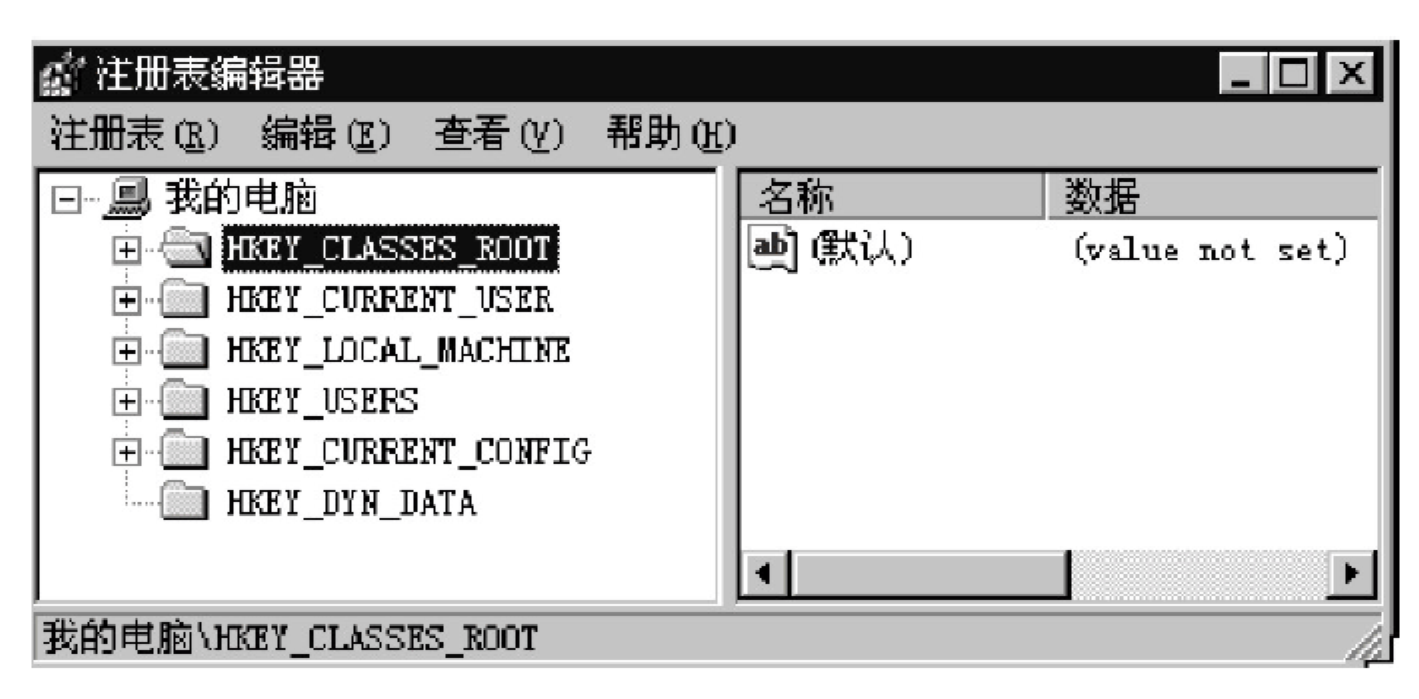


图14-13 运行regedit.exe后的"注册表编辑器"窗口

② 在"运行"窗口的"打开(O):"文本框内,如果键入程序的名称为regedit32.exe,单击"确定"按钮后,则激活与图14-13类似的一系列窗口。

由于注册表中包含了计算机运行需要的重要信息,因此,最好使用Windows NT系统的其他功能工具来控制、更改系统的设置。除非绝对必要,请不要编辑注册表。如果注册表中出现错误,计算机可能无法正常运转。一旦发生这种情况,请将注册表还原为上次成功启动时的状态。

(2)"注册表编辑器"数据的导出

在"注册表编辑器"中,可以将全部或部分注册表数据导出到文本文件中,其操作步骤

如下：

① 启动“注册表编辑器”，激活如图 14-14 所示的窗口。



图 14-14　在“注册表编辑器”窗口中导出注册文件

② 在图 14-14 所示的窗口中，依次选择“注册表”→“导出注册表文件”命令选项，激活“导出注册表”窗口。

③ 在“导出注册表”窗口中的“文件名”处，输入注册表的文件名，例如 RGT_1126，然后单击“保存”按钮，完成“注册表导出”的任务。在该窗口的“导出范围”中，可以选择和执行如下操作。

- 若要备份整个注册表，应选中“全部”单选钮。
- 若要备份该注册表的某个特定分支，应选中“选定的分支”单选钮，并输入要导出分支的名称。

注意：如果需要，用户可以使用任何文本编辑器编辑由“导出”创建的后缀为 .reg 的文件，如上述操作导出的 RGT_1126.reg 注册表文件。

(3)“注册表编辑器”数据的导入

基于注册表文件的重要性，如果系统启动出现故障可以还原注册表。下面介绍利用导出的“注册表文件”修复系统的方法。

① 启动“注册表编辑器”，激活如图 14-14 所示的窗口。

② 在图 14-14 所示的窗口中，依次选择“注册表”→“导入注册表文件”命令选项，激活“导入注册表文件”窗口。在窗口中，可以使用“搜索”栏，查找和选择需要导入的注册表文件，例如：选定的注册表文件为原先导出的 RGT_1126.reg 文件，最后单击“打开”按钮，激活导入过程的进度图，稍候，完成注册表的导入任务。

14.5.4　利用“NT 启动磁盘”修复被损坏的 NT 系统

本节将介绍修复系统的另一种方法。当 Windows NT 计算机系统损坏而无法启动时，用户可以利用自己制作的“NT 启动磁盘”修复系统。

由于 Windows NT 系统很大，因此，无论使用哪一种修复方法，修复的内容都是有限

的。有时,可以使用几种方法对被损系统进行修复。

当用户系统的部分启动文件损坏时,例如:ntdetetect.com、boot.ini 或者是映射磁盘区(mirror set)故障时,可以使用“NT 启动磁盘”方法进行修复。因此,要事先制作好这个磁盘,以便系统破坏时使用。

1. “NT 启动磁盘”的制作方法

① 在需要制作“NT 启动磁盘”的计算机桌面上,双击“我的电脑”图标。

② 选择其中的软盘驱动器的图标(如 3.5 英寸软盘)后,依次选择“文件”→“格式化”命令,进行格式化磁盘的操作。注意,不能使用 DOS 系统格式化磁盘。

③ 依次选择“资源管理器”→“查看”→“选项”命令选项,在激活的窗口中的“隐藏栏目”下,选中“显示所有文件”单选项后,单击“确定”按钮。

④ 对于一般的 x86 型计算机,复制到制作的“NT 启动磁盘”中的文件有:ntldr、ntdetect.com、boot.ini、bootfont.bin(使得启动画面显示中文信息)和 ntbootdd.sys。

2. 使用“NT 启动磁盘”修复被损坏的 NT 系统

当系统遇到故障而无法启动时,使用“NT 启动磁盘”修复系统的步骤如下:

① 由于硬盘中的 boot.ini 文件的属性是隐藏、系统文件和只读,所以必须先利用“NT 资源管理器”修改其隐藏和只读的属性,使其具有可以修改的属性。

② 将所制作的“NT 启动磁盘”插入软盘驱动器中,从软盘启动 NT 系统。

③ 磁盘中的 boot.ini 会自动选取硬盘中的正确启动系统,并利用其启动系统。

④ 启动完成后,用户应将硬盘中的 boot.ini 文件的属性改回原来设置的隐藏、系统文件和只读的属性值。

3. 使用“NT 启动磁盘”的注意事项

在本地计算机上制作的“NT 启动磁盘”只能在本地计算机上使用,这点与“紧急修复磁盘”修复系统的方法完全不同。

习题

(1) 什么是数据保护? 被保护的数据有哪几种? 为什么说数据保护是非常重要的?

(2) 网络中数据定期备份的原因和目的是什么? 数据备份的最终目的又是什么?

(3) 在设计网络文件与数据备份系统时需要考虑的因素有哪些?

(4) 建立数据文件备份的策略是什么? 备份制度的基本内容有哪些? 什么是备份文件? 常见备份文件的类型有哪些?

(5) 常用的备份设备有几种? 各有什么特点? 应如何选择备份设备?

(6) 大、中、小型单位在选择存储介质时应该怎样考虑? 如何选择?

(7) 如何确定备份程序? 什么是第 3 方备份程序? 使用时应注意什么?

(8) Norton Ghost 2001 具有哪些功能和特点? 使用它可以完成哪些工作?

(9) 什么是整体、增量、差量、归档和日常备份? 各有什么特点?

(10) 备份计划制定的具体内容有哪些? 备份版本的数量应如何考虑?

(11) 应如何选择备份版本的存放位置?

(12) 网络数据文件备份的基本过程包括哪些内容?

(13) NT 备份程序的作用是什么? 它有哪些功能?

(14) 什么是容错? 容错技术可以解决和处理哪些常见问题?

(15) 什么是 RAID 数据冗余? 它是如何实现的?

(16) Windows NT 服务器支持的 RAID 数据冗余技术是软件技术,还是硬件技术?

(17) 在 Windows NT Server 中实现容错的工具是什么? 它有什么功能?

(18) Windows NT 中的其他数据保护方法有哪几种? 各适用在什么场合?

(19) 什么是注册表(registry)? 它的重要性表现在哪些地方?

(20) NT 注册表的设计目的是什么? 注册表(registry)的功能是什么? NT 注册表中的 5 项基本内容是什么?

(21) 为什么说不要轻易更改注册表? 一旦注册表被破坏,应如何修复系统?

(22) 如何使用注册表(registry)修复被损坏的 NT 系统? 它的主要步骤有哪些?

(23) 如何利用"上一次的正确系统配置"恢复 NT 系统? 使用它可以恢复些什么?

(24) 利用"NT 启动磁盘"修复被损坏的 NT 系统时,应该如何制作"NT 启动磁盘"?

实训题目

1. 使用 Ghost.exe 程序制作系统某一分区的整体备份,并在另一空白分区中恢复该备份。

2. 制作"NT 启动磁盘"并使用它引导本计算机系统。

3. 制作用于 NT 系统引导的"安装磁盘组"3 张软盘;制作"紧急修复磁盘"1 张;使用这 4 张磁盘和 NT Server(NT Workstation)CD-ROM 光盘,修复一台计算机的 NT 系统。

4. 制作一张"NT 启动磁盘",并使用它引导并修复被损坏的本机 NT 系统。使用"注册表编辑器"管理、导入和导出"注册表文件"。



第15章 网络安全管理

本章将介绍计算机和网络安全的基础知识，以及网络安全系统中常用的关键技术。其中包括：安全保护策略、防火墙技术、代理服务技术、网络防病毒技术等。这些技术都是网络管理员在设计和考虑网络安全体系时必须掌握的重点技术，也是网络安全保障的基础。在本章的最后，以 Windows NT 为例来说明网络操作系统中的安全体系和安全子系统，即身份验证系统、资源访问控制系统和安全审核系统。

通过本章的学习，可以对网络的安全基础知识有所了解，并进一步明确网络管理员在网络安全管理工作中的基本目标和职责，从而可以采用各种手段来确保网络系统的安全运行，以及数据资源的安全。

主要内容：

- 计算机网络安全概述；
- 计算机安全和计算机网络安全；
- 网络安全系统的关键技术和安全保护策略；
- 网络安全的评估标准；
- 防火墙技术和企业防火墙的构建；
- 代理服务技术和代理服务的应用；
- 网络防病毒技术，包括计算机和网络病毒的防治技术；
- 网络操作系统中的安全体系；
- Windows NT 4.0 的安全概述；
- Windows NT 网络安全子系统的实现。包括身份识别系统、资源访问权限控制系统和安全审核系统。

15.1 计算机网络安全基础

网络的安全技术是一门新型的迅速发展着的学科，许多方面还不是很成熟。为了适应计算机网络技术的发展，国际标准化组织制定了网络安全体系结构模型，该模型主要是解决网络系统中所传输信息的保密问题。目前，实际使用的计算机网络安全管理系统主

要包括对授权机制、访问机制和加密/解密机制的管理。在设计计算机网络的安全系统时，理论上是越安全越好，但实际应用时，不应一味地追求高安全性能，而应当针对不同计算机网络系统的安全要求，采取适宜的措施，使得网络系统的安全性能和价格的比值达到合理的水平。

网络管理员对网络系统的安全负有重要的责任，网络安全是网络管理中心的一项主要工作内容。网络管理员应当对网络结构、网络资源分布、网络用户类型与权限，以及网络安全的检测方法都了如指掌。当网络安全受到损害或出现问题的苗头时，网络管理员不但要有判断和预见能力，能够及时采取必要的预防措施，同时还应具有紧急情况下处理故障的能力。

计算机网络是由计算机为主的资源子网和通信设备及传输介质为主的通信子网两部分组成。因此，计算机网络的安全就是由这两部分的安全组成的。

15.1.1 计算机网络安全概述

随着 Internet 的发展，网络在为社会和人们的生活带来极大方便和巨大利益的同时，也由于网络犯罪数量的与日俱增，使许多企业和个人遭受了巨大的经济损失。利用网络进行犯罪的现象，在商业、金融、经济业务等领域尤为突出，例如，在网络银行和电子现金交易等场合，出现了多起由于网络犯罪而引发的银行倒闭的事件。

面对日益严重的危害计算机网络的种种威胁，人们认识到必须采取有效的措施来保证计算机网络的安全性。于是，世界各国纷纷颁布了计算机网络的安全管理措施和规定，我国也颁布了《计算机网络国际互联网安全管理办法》，用来制止网络污染，阻止危害国家安全、泄露国家机密、侵犯国家和他人利益的行为发生。计算机和网络的安全措施可以分为逻辑的、物理的和政策的 3 类。

15.1.2 计算机安全

1. **ISO 对计算机安全的定义**

国际标准化组织 ISO 对计算机安全的定义是：计算机安全是指为了保护计算机数据处理系统而采用的各种技术和用于安全管理的措施，其目的是为了保护计算机硬件、软件和数据不会因为偶然或故意破坏等原因遭到破坏、更改和泄露。

2. 计算机安全的内容

计算机安全应当包括如下主要内容：

① 计算机硬件的安全性　主要是确保计算机硬件环境的安全性。例如，确保计算机硬件设备、安装和配置，以及计算机房和电源等的安全性。

② 计算机软件的安全性　主要是保护计算机系统软件、应用软件和开发工具的安全，使它们不被非法修改、复制和感染病毒等。

③ 数据的安全性　就是保护数据不被非法访问，并确保数据具有完整性、保密性和可用性。

④ 计算机运行的安全性　是指计算机在遇到突发事件时为了保护系统资源而采取的措施。例如计算机遇到停电时的安全处理等。

3. 破坏计算机安全的途径

破坏计算机安全的途径有以下几种：

① 窃取计算机用户的身份及密码。例如窃取计算机用户名称和口令，并非法登录计算机，进而通过网络非法访问数据。例如非法复制、篡改软件和数据等。

② 传播计算机病毒。例如，通过磁盘、网络等传输计算机病毒。

③ 计算机数据的非法截取和破坏。例如，通过截取计算机工作时产生的电磁波的辐射线，或通过通信线路破译计算机数据。

④ 偷窃存储有重要数据的存储介质。例如光盘、磁带、硬盘和软盘等。

⑤ "黑客"非法入侵。例如，"黑客"通过非法途径入侵计算机系统。

4. 保护计算机安全的措施

保护计算机安全的措施有以下几种：

① 物理措施　包括计算机房的安全，严格的安全制度，采取防止窃听、防辐射等多种措施。

② 数据加密　对磁盘上的数据或通过网络传输的数据进行加密。

③ 防止计算机病毒　计算机病毒会对计算机系统和资源造成极大的危害，因此，防止计算机病毒是非常重要的防范措施，其主要措施是加强计算机的使用管理，选择较好的防病毒软件。

④ 采取安全访问措施　在各种计算机和网络操作系统中广泛采取了各种安全访问的控制措施。例如：使用身份认证和口令设置，以及数据或文件的访问权限的控制等。

⑤ 采取其他安全访问措施　为确保数据完整性而采用的各种数据保护措施、制订安全制度和加强管理人员的安全意识等。例如计算机的容错技术、数据备份和审计制度等。此外，还要加强安全教育，培养安全意识。

15.1.3 计算机网络的安全

1. 计算机网络安全

计算机网络安全是指通过采用各种安全技术和管理上的安全措施，确保网络数据的可用性、完整性和保密性，其目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

2. 计算机网络安全的定义

由于计算机网络组建的基本目的是向网络用户提供网络上的共享资源（软件、硬件和信息资源），并向网络用户提供各种类型的服务。因而网络安全的基本定义是：确保网络服务的可用性和网络信息的完整性。而最新的网络安全定义的特征是由美国计算机专家提出的安全框架所规定的，他们认为只有具有这样一些更多的性能才能解释网络中的各种安全问题。该框架包括如下性能特征：

① 保密性（security）　信息应具有不被泄露给非授权的用户、实体或过程，并被其利用的保密特性。

② 完整性（integrity）　数据具有未经授权不能改变的特性。即信息在存储或传输的过程中具有保证不被修改、损坏和丢失的特性。

③ 可用性(availability)　通常是指网络中主机存放的静态信息具有可用性和可操作的特性。当需要时,能够存取所需要的信息。

④ 实用性(utility)　即保证信息具有实用的特性。例如:信息的加密的密钥不可丢失或泄密。丢失了密钥的信息就丢失了信息的实用性。

⑤ 真实性(authenticity)　是指信息的可信度。即保证信息具有完整、准确、在传递和存储过程中不被篡改等特性,还应具有对信息内容的控制权。

⑥ 占有性(possession)　是指存储信息的主机、磁盘和信息载体等不被盗用,并具有该信息的占有权。即保证不丧失对信息的所有权和控制权。

3. 计算机网络中易受到威胁的网络资源

计算机网络中可能受到威胁和需要保护的网络资源有以下几种:

① 硬件设备　例如服务器、交换机、路由器、集线器和存储设备等。

② 软件系统　例如操作系统、数据库系统、应用软件和开发工具等。

③ 数据或信息。

4. 网络安全威胁的类型和有意危害网络安全的人

若想保证网络的安全,必须能够防范来自危害者的安全威胁。因此,网络管理员应当清楚网络安全威胁的类型和危害网络安全的人。

(1) 网络安全威胁的类型

在网络安全性中,人们将对网络安全造成的威胁分为两种类型。

① 有意造成的危害。

② 无意造成的危害。

(2) 有意危害网络安全的 3 种人

① 故意破坏者(hacker)　即网络"黑客",他们企图通过各种手段去破坏网络资源和信息,例如,篡改别人主页、修改系统配置与造成系统瘫痪等。

② 不遵守规则者(vandal)　他们企图访问不允许他们进入的系统。其目的有时只是到网络中看看;有时只是想盗用别人的计算机资源,例如 CPU 使用时间。

③ 刺探秘密者(cracker)　他们的目的非常明确,即通过非法的手段入侵他人的系统,进而窃取商业秘密和个人资料。

5. 攻击计算机网络安全的主要途径

① 通过计算机辐射、接线头、传输线路截取信息。

② 绕过防火墙和用户口令,进入网络,进行非法及越权操作。例如非法获取信息或修改数据。造成网络工作的混乱,甚至是严重的泄密事件。

③ 通过截获、窃听等手段破译数据。

④ "黑客"通过电话网络,非法尝试进入计算机网络。由于"黑客"具有较高的计算机知识和使用技巧,因此,他们在破译网络的口令之后,就可以以合法用户的身份进入并使用该系统,进而取得更高的权限,对网络进行全面的破坏。例如删除、修改网络中的数据资料等,致使网络部分或全部瘫痪。

⑤ 向计算机网络注入病毒,造成网络瘫痪。

6. 攻击计算机网络安全的方法和类型

① 假冒欺骗　假冒欺骗的常用方法有两种：其一，采用源 IP 地址进行欺骗性攻击，即入侵者伪装成来自内部主机的一个外部地点传送信息包，这些信息包中包含有内部信息的源 IP 地址。其二，在电子邮件服务器使用报文传输代理（MTA，message transfer agent）冒取他人之名窃取信息。

② 指定路由　发送方指定了信息包到达的路由，此路由是经过精心设计的，可以绕过设有安全控制的路由。

③ 否认服务　否认服务通常指对信息的发布和接收不予承认。

④ 数据截取　数据截取是网络上“黑客”和“间谍”常用的方法，他们先截取大量的信息包，而后加以分析，并进行解密，获取合法的密码。

⑤ 修改数据　修改数据就是非法改变数据的内容。

15.1.4　网络安全体系

为了适应网络技术的发展，国际标准化组织根据开放式系统互联参考模型 OSI 制订了一个网络安全体系结构模型，该模型主要解决网络系统中传输信息的安全和保密问题。这就是 ISO 7498-2 网络安全体系，它确定了多种基本安全服务和多种安全技术。

1. 网络安全体系所要求的 6 类基本安全服务

网络安全体系所要求的 6 类安全服务是：对等实体鉴别服务、访问控制服务、数据保密服务、数据完整性服务、数据源鉴别服务和禁止否认服务。

2. 网络体系的安全机制

为了实现安全服务，网络安全体系结构采用的安全机制有以下几种：

① 加密机制　确定对不同的信息类型采用和实施不同的加密措施，包括存放在存储媒体内的数据和需要进行传输的数据，它是提供数据保密的最常用的方法。例如：按加密算法的密钥类型分类，可以分为对称密钥加密算法和非对称密钥加密算法；按密码体制分类，可分为序列密码和分组密码两种。用数据加密的方法与其他安全技术相结合，可以保证数据的保密性和完整性。在 OSI 模型中，除了对话层不提供数据加密的保护外，其他各层都可以提供加密功能。另外由于密钥的重要性，加密机制中必须提供一套完整的密钥管理机制。

② 数字签名机制　数字签名机制是解决网络中特有安全问题的有效方法。例如使用 RSA 等公开的密钥算法生成一对公钥和私钥，信息发送时需用私人密钥加密（即签名），信息的接收者则利用信息发送者的公钥对签名的信息进行解密，以验证发送者的身份。

③ 标识与验证机制　主要指对用户身份的标识与鉴别。例如：使用用户名加上口令是最基本的方法，也是网络访问控制机制的基础。

④ 网络访问控制机制　主要指对具体的各个用户给予必要的授权，允许或限制其访问存取的范围、方式、时间、地点和可采用的操作等。通常应根据本单位的安全策略进行设置。

⑤ 信息完整性机制　主要指判断并确认数据或信息在存储或传输过程中是否被篡

改或破坏。通常加密机制与信息完整性机制都是采用密码技术来实现的。

⑥ 认证和审计机制　确认接收到的信息的真伪,监视与记录对网络的访问,发现或预防网络安全性方面的漏洞。

15.1.5 网络安全的评估标准

随着计算机和网络安全问题的日益突出,计算机和网络的安全性能逐步为人们所重视。人们在建立网络的同时,也越来越多地关注计算机和网络具有的安全性能。因此,建立完整、客观的评价标准也成为各国关注的热点问题。1983 年美国国防部率先提出了一套《可信计算机评估标准》,它将计算机系统的安全等级划分为 A、B、C、D 4 大类 7 个小类,包括了从最简单的系统安全特性直到最高级的计算机安全模型技术。目前,这套评估标准常为广大的网络管理人员所引用,本小节将分别进行解释。

1. D 级

D 级是最低的安全保护级。拥有此级别的系统,不具有任何保护措施,任何人都可以自由进出系统,没有任何系统和数据访问的限制。属于这个级别的操作系统有:DOS、Windows 和 Apple 的 Macintosh System 7.1 等。

2. C1 级

C1 级又称选择安全保护级,它描述了一种典型的用于 Unix 系统上的安全级别。这种级别的系统对硬件具有某种程度的保护,但硬件仍然具有受到损害的可能性。用户拥有注册账号和口令,系统通过账号和口令来识别用户是否合法,并决定用户对程序和信息拥有的访问权。但这种系统的缺陷是不能控制进入系统的用户的访问级别,因此,用户不但可以将系统中的数据任意移走,还可以控制系统配置,从而获取此系统管理员允许的最高级别。例如,自行更改用户名和口令。

3. C2 级

C2 级又称受控的安全访问控制级。它除了包含 C1 级的特点以外,还具备访问控制环境。该环境具有进一步限制用户执行某些命令或访问某些文件的权限,而且还加入了身份验证级别。此外,系统可以对发生的事件进行审计工作,并写入日志。例如,计算机何时开机,用户的登录地点,登录的成败与否,系统管理员执行命令的情况,以及身份的验证等均可以记录在案。审计的缺点是需要耗费系统的硬件资源,例如 CPU 的处理时间和硬盘的存储空间。能够达到 C2 级别的操作系统有:UNIX、Windows NT/2000 和 Novell 3.x 等操作系统。

4. B1 级

B1 级为标志安全保护级,是支持多级安全的第 1 个级别,该级别除了具有 C2 安全级别的特点之外,还增加了安全策略模型、托管访问控制和数据标志等特性。具有此级别的系统是具有保密和绝密的系统。该系统的对象处于强制性访问控制之下,系统不允许文件的拥有者改变其许可权限。例如,国防部和国家安全机构的计算机系统,一般该系统的所有者为政府机构和安全防御的承包部门。

5. B2 级

B2 级为结构化安全保护级,该级别的设计方案,在设计时就必须具有一个整体化的、

合理的、面向安全的体系结构。应当遵循最小授权的安全原则,具有良好的抗渗透能力,并对所有的主体和客体进行访问控制型的保护等。例如,要求计算机系统中所有的对象都加标签,而且给设备(磁盘、磁带和终端等)分配单个或多个安全级别。

6. B3 级

B3 级为安全域机制安全保护级,该级别的系统具有安全内核和高抗渗透能力,使用安装硬件的方式来加强域。该级别要求用户通过一条可信任的途径连接到系统上。例如,使用内存管理硬件来保护安全域内的对象不受非法访问,或避免对其所做的非法修改等。

7. A 级

A 级为可验证的安全设计保护级。它是当前的最高安全级别,包括了一个严格的设计、控制和验证过程,这一级别包含了较低级别的所有特性。设计必须是在数学角度上经过验证的,而且必须进行秘密通道和可信任分布的分析。该信任分布的含义是:为了实现安全系统的保护,被保护系统的硬件和软件在物理的传输过程中均应受到保护。

注意:由 C2 开始的每一级别都拥有较低一级的所有特性,并在此基础上增加了新的安全特性。例如,C2 级别除了包含 C1 级别的安全特性,还增加了身份验证和审计等。

15.1.6 网络安全保护策略

所谓安全保护策略是指一个网络对安全问题所采取的原则,对安全使用网络资源的具体要求,以及保证网络系统安全运行的措施。常用的网络安全保护策略有以下几条。在实际的网络安全系统中,应尽量遵循这些原则和策略。

1. 最小特权(授权)原则

最小特权原则是指对任何一个系统而言,其对象应该只具有履行其职责(执行特定任务)所需要的最小的权限。此处的对象可能是用户、管理者、程序或系统。最小特权原则的使用可以尽量限制系统对入侵者的暴露,以减少由此可能带来的破坏。在网络环境中,最小特权原则被大量地使用。

① 首先,并非每位系统管理员都需要知道系统管理员的口令(即根口令),因此,只将根口令告诉需要的管理人员。其次,对于知道根口令的管理员来说,并不是执行每项操作时都需要最高的操作权限,因此,可以为该管理员建立多个账户,当他进行一般工作时,只用一般权限的账户注册。

② 在 Intranet 的包过滤型防火墙系统中,应当将其设计成只允许需要的 Internet 网络访问和服务的进出,而不是允许所有的访问和服务进出。

在执行最小特权原则时应当注意两个问题:其一,确认成功地应用了最小特权原则;其二,不能因为最小特权的使用而影响用户或系统的正常工作。

2. 纵深防御

纵深防御是指系统中应当使用多种安全机制,而不要仅依赖一种安全机制。这样可以实现多种安全机制的互相支持,提供有效的冗余技术,以防由于一种机制的失效,而引发的危害。因此,这也是基本的安全设计原则。例如在 Intranet 中建立了防火墙系统的同时,还可以使用主机安全的防御技术,以及加强安全教育和系统安全管理等。

3. 阻塞点

阻塞点是指可以对攻击者进行监视和控制的一个狭小的通道。例如在 Intranet 中，内部网络与 Internet 之间的连接如果只有防火墙，则防火墙就是一个阻塞点。因为，任何想从 Internet 上攻击 Intranet 内部网的入侵者必须通过这个通道。用户可以通过对阻塞点的观察，发现攻击者的企图，并及时做出相应的反应。

值得注意的是：倘若攻击者采用其他的办法绕过了阻塞点，则阻塞点就失去了作用。例如，当网络中存在有多条电话拨号连接时，防火墙并不能阻止所有线路的攻击。因为，攻击者有时可以仅通过一个次级的连接，或一个间接的连接而进入网络，从而给网络带来破坏。

4. 最薄弱连接点

在设计网络时，应当尽量避免最薄弱连接点，因为，最薄弱连接点直接决定了系统连接的强弱，防火墙的强弱也取决于最薄弱连接点。对于无法消除的最薄弱连接点，要严加防范。因此，在设计网络的安全系统时应均衡处理各个环节，不应有所偏重，导致最薄弱连接点的出现。

5. 失效保护

安全失效保护原则也是安全保护的一个普遍原则。其含义在于：即使安全保护失败，也应保证系统的安全。在应用失效保护原则时，可以使用默认拒绝和默认许可两种设置准则。虽然失效保护能够将攻击者拒之于门外，但是也会因此而拒绝合法的用户。

(1) 默认拒绝

从安全角度看是一种安全的失效保护状态，它是指在安全保护失败时，只允许执行预先决定的服务，而禁止除此之外的所有服务。预先决定的服务是根据用户和网络安全的需要而逐步确定的。对于那些不能安全地用现行方式提供的服务，可以将其限制在部分用户或系统中。

(2) 默认允许

默认允许是预先决定需要禁止的服务，它是指在安全保护失败时，除了禁止的服务之外都是被系统允许的。因此，预先禁止的服务应当尽量保证系统的安全。这种方式将增加防火墙管理者和用户之间的矛盾，因为，系统维护者会逐步将一个个不安全的服务点加入到预先禁止的范围内，而用户总是想获得尽可能多的服务。

6. 普遍参与

网络系统的安全需要全体人员的普遍参与。例如，网络中的每个人均应及时报告与系统安全有关的异常事件，还需要配合管理员定期更换口令，自觉维护系统的安全。

7. 防御多样化

防御多样化是指在一个系统中使用多种类型的安全机制，这样可以避免攻击者侵入一个安全系统就能够轻而易举地侵入整个系统。防御多样化还可以减少因为一个普通的、小型的、配置型错误而危及整个系统安全的可能性。但是，防御多样化会增加系统管理的复杂性，并增加管理员额外的时间，耗费更多的精力。

15.2 防火墙技术

防火墙是一种有效的网络安全机制。它是网络安全的屏障，通常由硬件和软件系统组合而成。本节将介绍有关防火墙的基础知识和实用技术要点。

15.2.1 防火墙基础

1. **防火墙(firewall)的作用和特点**

防火墙通常设置在“被保护网络”(LAN 的内部网络)与外网(Internet)之间，如图 15-1 所示。一个防火墙可以是一个路由器、一台主机、或者是一个主机群。

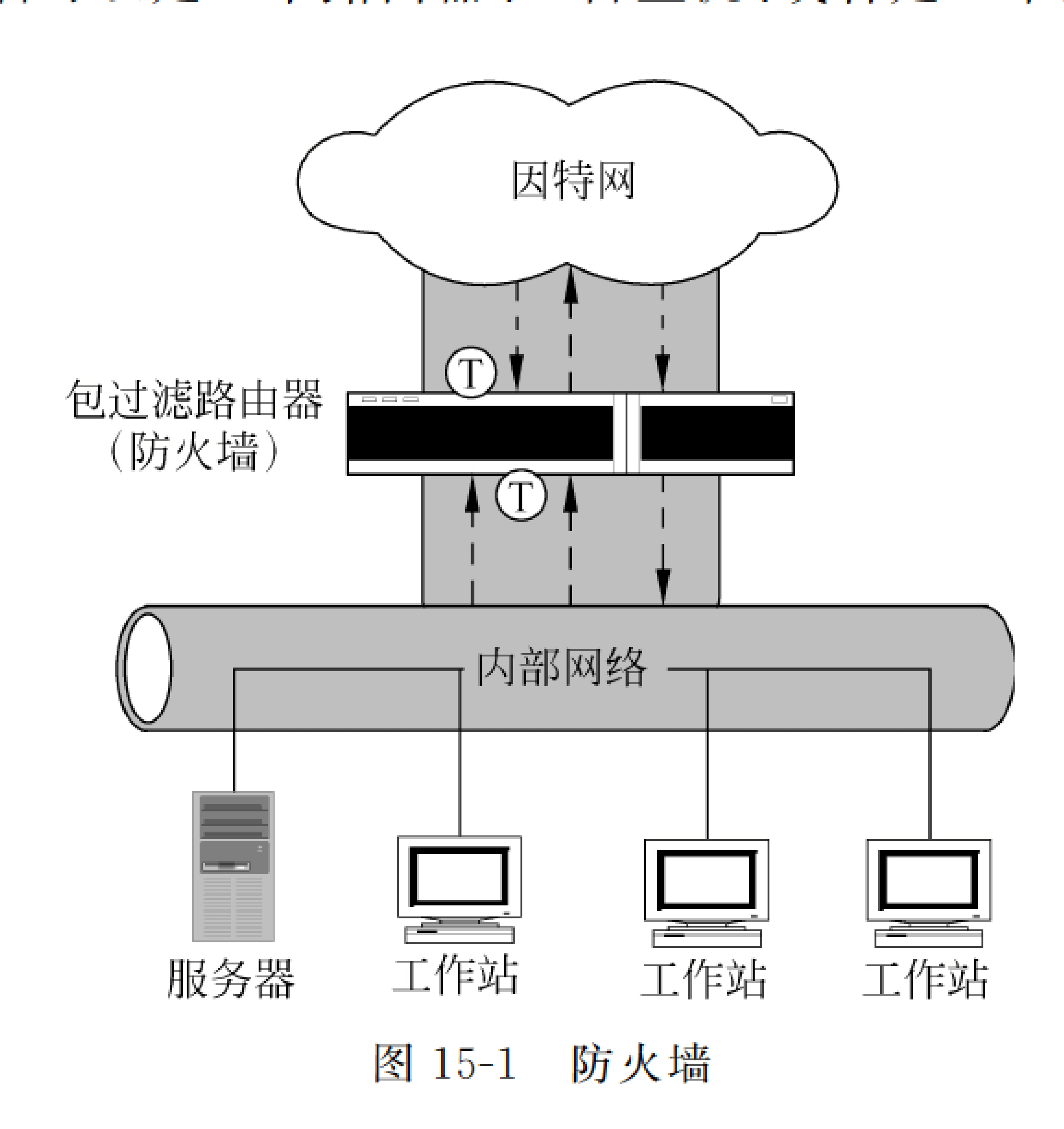


图 15-1 防火墙

(1) 防火墙的主要作用

防火墙通常被安装在被保护的内网与因特网的连接点上。建立防火墙的主要目的是为了防止“被保护的网络”受到来自外网(Internet 或其他外部网络)的入侵、干扰和破坏。其主要作用如下：

① 限制用户或其他人员必须从一个严格控制的点进入 Intranet 的内部网络，例如，使用远程登录 Telnet 命令登录内部网络。

② 限制内部网络中的用户必须从一个严格控制的点离开，例如，Intranet 的内部用户使用 Internet 上的电子邮件、WWW 浏览和 FTP 访问等。

③ 防止进攻者接近其他防御设备。

(2) 使用防火墙的特点

① 优点。

- 可以强化安全策略　防火墙可以根据安全策略规定的规则，仅仅允许“许可的服务”通过与授权的用户通过。因此，可以有效地控制用户的访问。
- 记录网络活动　作为内网进入和离开的惟一点，防火墙可以收集并记录内外网络

之间的联系、网络使用情况和错误信息。

- 限制内网段用户之间发生的问题影响到全局　由于防火墙能够隔离开各个网段，因此，可以有效地防止内网所发生的局部安全问题影响到全局网络。
- 集中有效的安全策略　作为网络信息的出入点，防火墙可以将网络安全和防范的策略与功能集中在一起，成为网络的安全屏障。

② 缺点。防火墙仅仅解决了网络安全防范的问题，但它不能解决如下问题：

- 不能防范恶意的知情者　对于已经进入网络的人为破坏，防火墙无能为力。
- 不能防范不通过它的连接者　防火墙可以有效地防止通过它的信息，但是不能防止那些不通过它，绕过它传输的信息，例如：内网计算机用户使用 modem 时的非法入侵的攻击信息。
- 不能防范全部的威胁　对于已经设计好的防火墙防御方案，防火墙只能用来防范已知的威胁，不能防御那些未考虑到的威胁。
- 不能防范病毒　防火墙不能防范网络上通信微机上的病毒，只能在防火墙后面杀灭病毒。

2. 防火墙建立的基本准则

防火墙建立的基本准则基于上述的失效保护原则，它有以下两种建立方式：

(1) 未被允许的就是禁止的

基于这个准则建立防火墙时，应当首先封锁所有的信息流，然后，再对希望提供的服务逐一开放。这种防火墙的弊端是限制了用户对服务的使用。

(2) 未被禁止的就是允许的

基于这个准则建立防火墙时，应当首先开放和转发所有的信息流，然后，再逐一禁止可能有害的服务。基于这个准则建立的防火墙的弊端是随着网络提供服务数量的增加和受保护网络范围的逐渐扩大，所提供的网络安全防护将越来越不可靠。

3. 防火墙的基本类型

防火墙的基本类型有以下几种：

① 数据包过滤型　除了专用的包过滤防火墙外，一般将数据包的过滤规则安装和设置在路由器上，其过滤规则是以 IP 数据报信息为基础的，可以实现对 IP 源地址、IP 目的地址、端口和封装协议等的过滤。数据包过滤在 OSI 模型的网络层上进行。

② 代理服务型　代理服务型防火墙通常以客户/服务器模式工作，因此，由服务器端和客户机端程序共同组成。

③ 复合型　复合型防火墙是数据包过滤和代理服务两种类型防火墙的组合形式，通常由堡垒主机提供代理服务。复合型防火墙的常见类型有以下几种：

- 双宿主机防火墙；
- 主机过滤防火墙；
- 加密路由器防火墙。

15.2.2 企业防火墙的构建

1. 与防火墙有关的基本术语

为了构建实用的防火墙，网络管理员应当首先了解与防火墙有关的基本知识，下面简单介绍如下一些概念和术语：

(1) 防火墙

限制被保护网络与因特网之间或其他网络之间信息访问的部件(硬件及软件)或部件集。建立防火墙的主要目的是防止需要保护的子网受子网之外因素的干扰和破坏。

(2) 主机

主机就是连接到网络上的任何计算机系统。

(3) 堡垒主机

一个暴露于外部网络(因特网)上，同时又是内部网络用户的主要连接点的计算机系统。堡垒主机极易受到侵袭和损害。

(4) 双宿主主机

双宿主主机，又称双重宿主主机，简称双宿主机。该主机是具有至少两个网络接口(或宿主)的计算机系统。

(5) 数据包

数据包是使用 TCP/IP 协议的 Internet 和 Intranet 上传输的基本信息单位。

2. 网络中常用的安全机制

防火墙系统中的常用实现技术包括分组过滤、应用网关和代理服务。

(1) 分组(包)过滤技术

分组过滤又称包过滤，它是一种基于路由器的技术。包过滤路由器对通过它的 IP 数据分组进行选择和过滤，允许或拒绝特定的数据包通过。

① IP 分组过滤的作用域。

过滤的规则一般基于 IP 数据包的下列各域：

- IP 数据包的源地址；
- IP 数据包的目的地址；
- TCP 或 UDP 协议的源端口号；
- TCP 或 UDP 协议的目的端口号；
- ICMP 消息类型；
- 封装协议或服务类型的选型，例如 TCP、UDP 或 ICMP 等。

基于源/目的 IP 地址的过滤是指根据网络的安全准则过滤掉具有特定 IP 地址的分组，从而达到保护内部网络的目的。而基于 TCP/UDP 源/目的端口号的包过滤提供了更大的灵活性，因为，端口号可以区分不同的服务类型或连接类型。例如，SMTP 使用端口 25，Telnet 使用端口 23，如果在包过滤路由器中禁止 25 和 23 端口的 IP 分组的进入，就可以防止黑客利用该服务对内部网络的攻击。常见的服务与标准(默认)端口编号见表 15-1。

② 采用分组过滤技术的特点。

表 15-1　网络中常用的服务、协议和系统默认的端口号码

名　称	服务方式	默认端口编号
HTTP	超文本传输协议	80
FTP	文件传输协议	20/21
Telnet	远程终端登录协议	23
SMTP	简单硬件传输协议	25
SNMP	简单网络管理协议	161/162
DNS	域名解析服务协议	53
POP	邮件接受协议	110
SOCKS		1080
…		…

优点：手段简单、效率高、速度快、实现方便和价格低廉，对于用户来说，不必进行技术培训，也不必在每台主机上安装特定的软件。

缺点如下：

- 由于数据包过滤规则的定义比较复杂，网络管理员需要对各种 Internet 服务、包头的格式、以及包的每个域均非常熟悉，因此，包过滤防火墙的维护比较困难。
- 难于抵御地址欺骗等攻击。例如，只能阻止一种类型的 IP 欺骗，即外部主机伪装成内部主机的 IP，而不能制止外部主机伪装成其他可信任的外部主机的 IP 欺骗，因而，安全性能较差。
- 任何直接经过路由器的数据包都有被用做数据驱动式攻击的潜在威胁。
- 一些包过滤型网关不支持有效的用户认证。因为，用户认证是可以伪造的。因此，没有基于用户的认证，仅通过 IP 地址的判断是不安全的。
- 审计功能差。不能提供有用的日志。
- 随着过滤规则数目的增加，由于需要执行所有的过滤规则，而消耗了 CPU 的时间，降低了系统的性能，使得过滤的路由器吞吐量下降。

(2) 应用网关技术

应用网关建立在网络的应用层，通常由一台专用的计算机来实现，其实质是软件防火墙，是工作在应用层的过滤器。应用网关根据特别的网络应用服务指定数据的过滤逻辑，并依据该逻辑对进出内部网络的数据进行过滤。应用网关逻辑可以对数据包的分析经过和采取的措施进行登记，以供统计和分析之用。应用网关的过滤机制需要为每个网络应用提供控制码，因此，它的效率较低，却较为安全。与包过滤路由器相比，采用应用网关技术具有如下特点：

① 优点　功能强、稳定性高、安装和配置方便、对网络速度无明显的影响、可以对分析的结果进行记录，以供进一步分析。由于它本身没有 IP 地址，因此，不易受到攻击，安全性较过滤路由器高；安装之后对整个网络的配置无影响，接通即可工作。例如：瑞星防火墙和天网防火墙都是此类的产品。

② 缺点　效率低；对满足过滤条件的数据允许通过，并建立其内部网络与外部网络的直接连接，此时，外部用户就能通过防火墙了解到内部网络的状况，从而威胁内部网络

的安全。

（3）代理服务技术

分组过滤和应用网关技术存在的共同缺点是当过滤条件满足时，防火墙内外系统将直接建立起连接，从而导致网络的安全性降低，为了克服这种缺陷，可以引入代理服务技术。代理服务器一方面代替原来的服务程序与客户程序建立连接；另一方面，也可以代替原来的客户程序与服务器建立连接。它确认内部用户的服务请求，并送达外部服务器；同时又将外部服务器的响应送回给内部用户。

（4）复合技术

在实际中，并非仅仅使用某项单独的技术来建立完整的防火墙。需要根据网络和安全的实际问题的要求来确定，如向用户提供的服务和安全保护等级的要求等。目前，实用的防火墙多数是代理服务技术和数据包过滤技术的复合型技术。

3. 常见防火墙的构建技术

本节将介绍常见防火墙的类型，以及它们的工作原理与实施和设计的要点。

（1）包过滤型（packet filter）防火墙。

① 结构与名称。

“包过滤型防火墙”又被称为“筛选路由器”或“分组过滤”防火墙，由于它一般工作在网络层（即 IP 层），因此，又名“网络层防火墙”或“IP 过滤器”，其连接方式如图 15-1 所示，主要部件是用于包过滤的路由器。

② 作用原理。

包过滤路由器的核心就是对包过滤算法进行设计，对进出内部网络的信息进行分析，并按照预定的安全策略，即信息过滤规则进行限制，允许授权的信息通过，拒绝非授权信息通过。信息过滤规则是以收到的数据包信息为基础的，当设定之后，如果数据包满足过滤规则，则允许它通过，反之，拒绝该数据包通过，相当于此数据包与其目的网络之间被断开，从而起到了保护内部网络的目的。

③ 采用包过滤技术的防火墙的特点，参见前面的“分组（包）过滤技术”。

④ 包过滤防火墙适用的场合。

IP 包过滤路由器无法对网络上流动的所有信息进行全面的控制，它不能理解特定的服务、环境和数据，因此，它适用于小型的、要求不高和投资较小的内部网络，对于这类网络具有以下一些要求：

- 机构是非集中化管理。
- 机构中没有强大的集中安全策略。
- 网络中的主机数目较少的场合。主要依赖于主机安全来防止入侵，而当主机数量增加到一定的程度时，仅靠主机安全是不够的。
- 没有使用 DHCP 这样的动态 IP 地址分配协议和管理的场合。

⑤ 包过滤路由器常用的过滤规则。

包过滤防火墙的核心就是对包过滤算法的设计，根据路由器的类型，包过滤的规则可能在输入或输出时进行。常见的包过滤规则有以下几项：

- 过滤规则号　FRNO，filter rule number。它决定过滤算法执行时过滤规则排列

的顺序，而正确地排列过滤规则是至关重要的事情。

• 过滤方式　包括允许(allow)和阻止(block)。
• 源 IP 地址　SIP，source IP address。
• 目的 IP 地址　DIP，destination IP address。
• 源端口　SP，source port。
• 目的端口　DP，destination port。
• 协议标志　PF，protocol flags option。
• 注释　即 comment。

⑥ 包过滤的规则制订过程。

• 明确网络的安全需求，确定包过滤的安全目标。首先明确被允许的和被禁止的是什么，然后制订合适的安全策略。
• 必须正式规定允许的包类型、包字段及其逻辑表达式。
• 使用防火墙支持的语法书写表达式。

(2) 双宿网关型防火墙

① 双宿网关防火墙的结构与工作原理。

在实际网络安全的设计中，人们为了弥补包过滤防火墙的不足，在包过滤防火墙的基础上加入了应用网关技术(代理服务器)作为补充，这就是如图 15-2 所示的双宿网关防火墙。这种防火墙系统的包过滤路由器放置在内部网络和 Internet 之间；而应用网关(代理服务器)则是配有两个网卡的主机系统，由于应用网关主机与内部网络同处一个网络，因此，它是外部网络用户进入内部网络的惟一通道和网络安全的要素。内部主机通过应用网关上的代理服务器得到 Internet 上的服务。入侵者则无法进入受到双重保护的内部网络，而外部网络用户又可以直接得到有效、合法的信息服务。

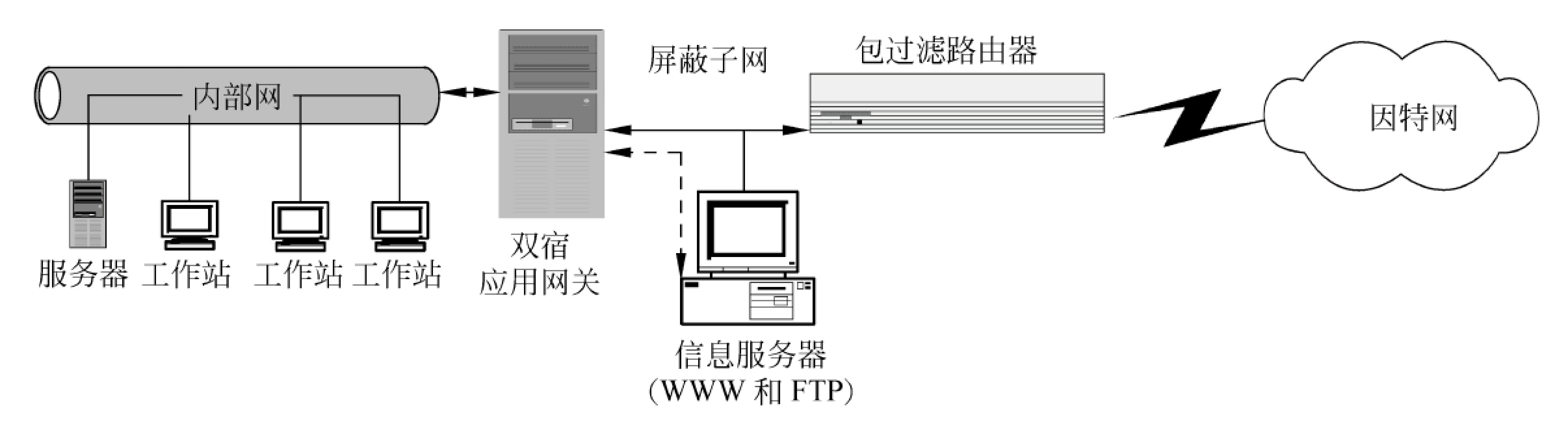


图 15-2　双宿网关防火墙

② 双宿网关防火墙的设计要点。

• 该结构使用一个单独的包过滤路由器提供筛选和过滤的功能，它被安置在外网与屏蔽子网之间。对外，应当注意在包过滤路由器上禁止外部登录应用网关(也称双宿网关)，以减少外部攻击的危险。如，应禁止远程客户使用 Telnet 协议登录到应用网关。对内，需要进行过滤规则的位置，使所有的通信路由到包过滤路由器，这样可以强制内部用户必须通过代理才能访问 Internet。
• 双宿网关型防火墙中的屏蔽子网是为向外部用户提供企业的一些特定的信息服

务而设计的，因此，应用时应当将 WWW、FTP 和 Gopher 等一些信息服务器设置在屏蔽子网内。

- 如果确实需要远程用户登录和注册到双宿(应用)网关主机，也应尽量减少应用网关上用户账户的数目。

③ 采用双宿网关防火墙的应用特点。

- 优点：由于这种防火墙实现了网络层(包过滤)和应用网关(代理服务)的双重安全保护，因此，它比包过滤防火墙具有更高的安全性能。此外，这种防火墙还提供了对外公开的信息访问服务，如 Wet 和 FTP 等。
- 缺点：第一，双宿网关防火墙的配置较为复杂；第二，由于双宿网关是能从 Internet 访问内部系统的惟一通道，如果允许远程用户的登录注册，就需要在它的上面创建多个用户账号，这些账号的存在为入侵者提供了相对容易的入侵方法和通道，由此会导致安全性降低。因此，为了保证内部网络的安全，这种防火墙通常不允许远程用户登录和注册到双宿主机，直接访问内部网络，因而，导致系统的灵活性下降。所以，这种防火墙不适合灵活性要求较高的场合。

(3) 屏蔽主机(screened host)防火墙

① 结构与工作原理。

屏蔽主机防火墙也被称为“被屏蔽主机”、“被甄别主机”、“堡垒主机”或“主机过滤”防火墙。它的连接方式如图 15-3 所示，这是一种更加灵活的防火墙配置方案。该结构的防火墙中，提供安全保护的主机仅与内部网络相连。另外，该结构中的包过滤路由器屏蔽掉可能危险的网络连接，并将所有许可的网络应用性服务转向堡垒主机，并通过该主机实现

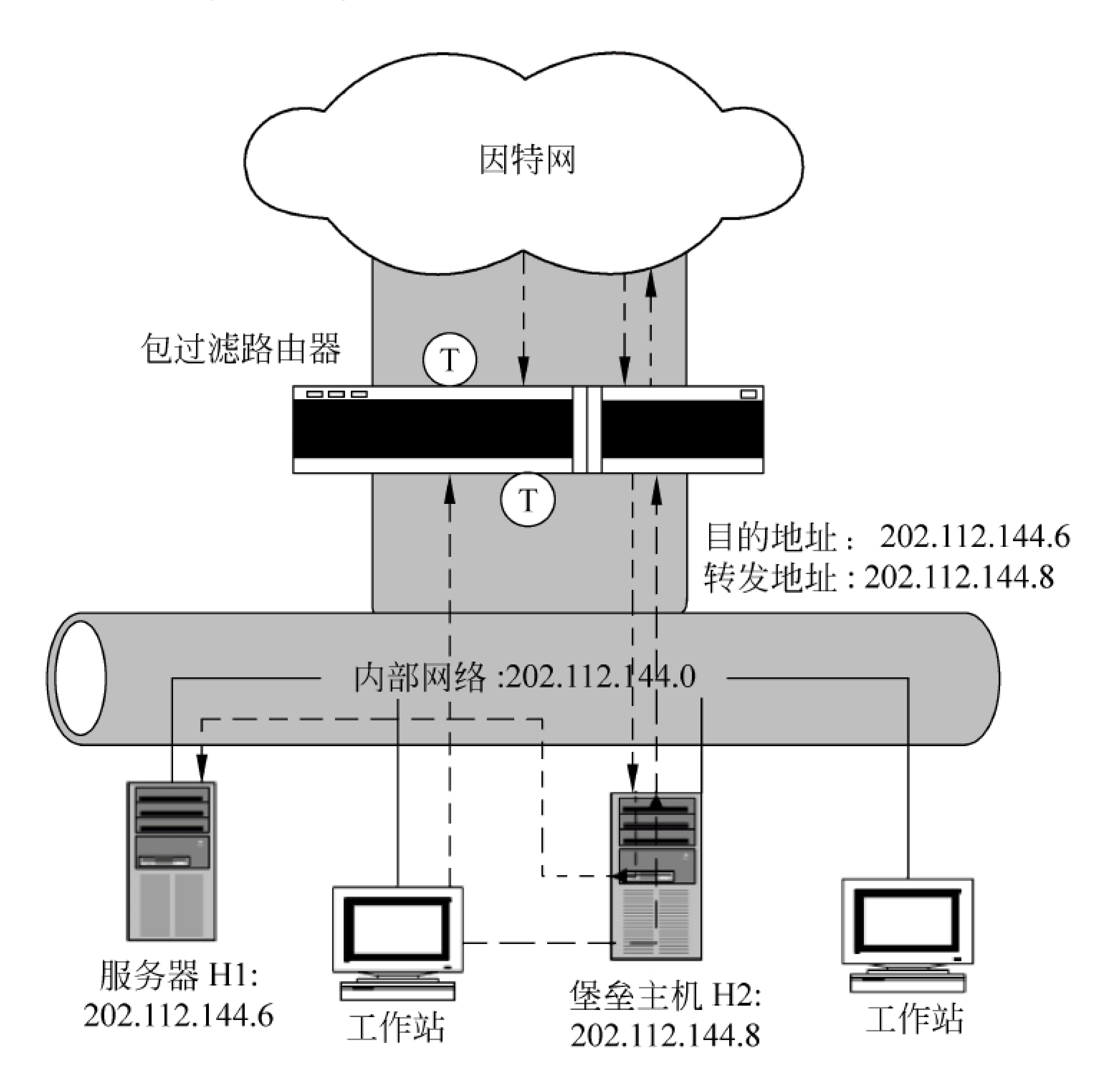


图 15-3　屏蔽主机防火墙

代理服务。

② 屏蔽主机系统中包过滤路由器的设计要点。

- 对安全要求较高时，使得任何外部网上的主机只能与堡垒主机建立连接。例如：可以将图 15-4 所示的路由器设置为不允许来自内部主机与外部主机的任何直接连接。
- 在应用要求更灵活的场合，以及堡垒主机许可的情况下，允许内部主机与 Internet 之间的某些类型的直接服务。例如：可以在路由器上进行设置，允许内部的其他主机（非堡垒主机）可以因为某些类型的服务请求与外部网络建立直接的连接。
- 禁止外网与堡垒主机的某些危险连接。例如禁止外部主机远程登录到堡垒主机。

③ 屏蔽主机系统中堡垒主机的设计与配置的要点。

被屏蔽主机系统中的堡垒主机向外部或内部客户程序提供网络服务，它具有多种身份，例如，它可能是邮件服务器、打印服务器、本地网络的 DNS 服务器和文件服务器等。因此堡垒主机的安全配置尤为重要，也关系到整个防火墙的安全。

下面简单介绍在 Intranet 中堡垒主机的配置要点。

- Telnet 服务　对 Telnet 服务的过滤一般应该通过包过滤路由器来实现。虽然使用代理实现该服务的过滤也可以，但是代价昂贵，因此不可取。
- FTP 服务　如果需要支持内部用户的普通 FTP 服务，可以在堡垒主机上建立代理，但是，应当注意禁止堡垒主机的匿名 FTP 登录。
- SMTP 服务　进入的邮件应当通过 DNS MX 记录引导到堡垒主机上，外出的邮件则应当通过堡垒主机发出，让邮件直接进入内部主机系统是不合适的做法。
- HTTP 服务　可以通过包过滤来提供，或者通过代理服务器间接实现。更安全的做法是通过带缓冲的代理服务器（CERN HTTP 服务器）来间接地提供。
- DNS 服务　主 DNS 服务器应当位于堡垒主机上，而内部网络内应当设有一个外部的次（secondary）DNS 服务器。如果堡垒主机是内部与外部的主 DNS 服务器，就不能隐藏任何信息。

④ 屏蔽主机防火墙的安全特性。

屏蔽主机防火墙强迫所有外部主机与堡垒主机相连接，而不允许外部主机与内部主机直接相连。这种结构由包过滤路由器和堡垒主机两级安全屏障组成，既实现了网络层的安全（包过滤），也实现了应用层的安全（代理服务），因此，这种结构的防火墙所能达到的安全等级比包过滤防火墙高。

由屏蔽（过滤）路由器提供主要的安全服务。在内部网络中，堡垒主机是惟一的连接点，若该计算机系统被入侵，则内部网络上的其他主机将失去安全保护。被屏蔽主机防火墙的特点如下：

- 优点　具有两道安全屏障，因此，该类型的防火墙的安全性能比包过滤路由器和双宿主机型防火墙更高。
- 缺点　这种防火墙的堡垒主机是内部网络的安全关键，一旦堡垒主机被入侵者攻克或破坏，内部网络则再无遮拦；其次，该结构的配置较为复杂。

（4）屏蔽子网（screened subnet ）防火墙

屏蔽子网防火墙也被称为“被屏蔽子网防火墙”和“子网过滤防火墙”，它支持两个网络层（过滤路由器）和一个应用层（堡垒主机的代理服务）的安全功能。

在屏蔽主机防火墙中，堡垒主机最容易受到入侵者的攻击。另外，由于其内部网络对堡垒主机是完全公开的，因而，一旦堡垒主机被攻克，则入侵成功。对于安全性要求较高的场合，应当选择安全性更高的被屏蔽子网防火墙。

① 结构与工作原理。

屏蔽子网防火墙的连接方式如图 15-4 所示，该结构是在屏蔽主机防火墙结构的基础上，添加了周边网络（屏蔽子网）而形成的。屏蔽子网防火墙可以进一步隔离内部网络与外部网络，并且减小堡垒主机被入侵的危险。

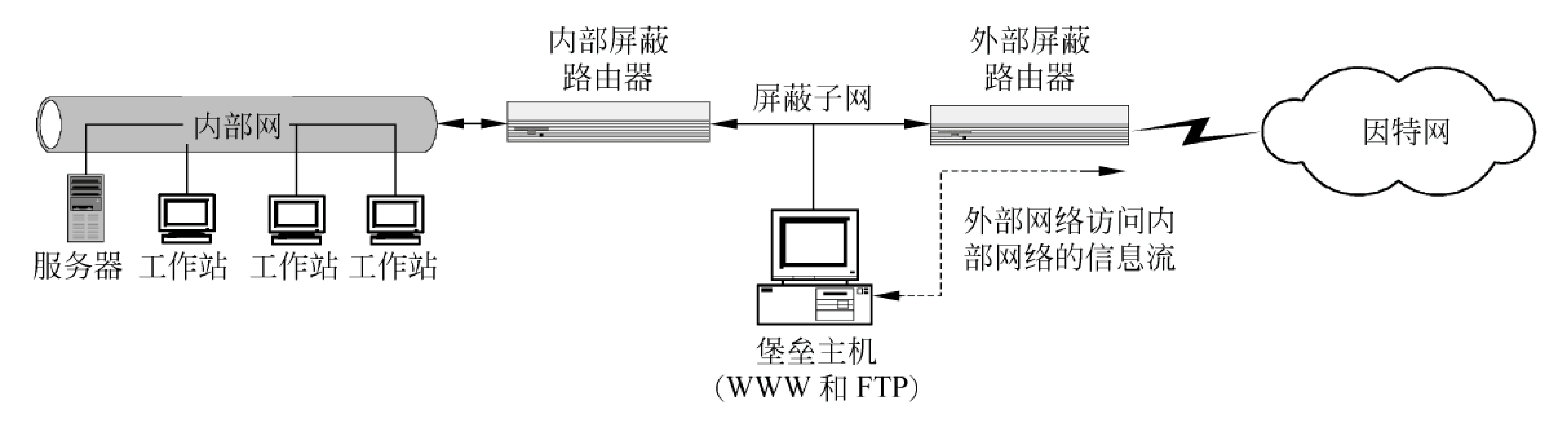


图 15-4　被屏蔽子网防火墙

当周边网络上的堡垒主机或 DMZ 被入侵时，入侵者只能探听出周边网络上来往于 Internet 的通信，而不能侦听到内网上的数据。这是因为，内部网络上的数据包，虽然在内网上是广播式流动的，但受内部路由器过滤规则的限制，这些数据包是不会流入周边网络的，因此，内部网络是安全的。

② 工作原理与设计要点。

ⓐ 周边网络。周边网络也叫非军事区 DMZ，de-militarized zone，或者是屏蔽子网，一般设置在被保护网络与外部网络之间，是能够提供安全保护的附加网络。如图 15-5 所示，DMZ 由两个包过滤路由器和一个堡垒主机组成。由于这个防火墙由多重安全防御系统组成，因此，它是目前最安全的一种防火墙。

- 设计时，网络管理员应当将堡垒主机、信息服务器、调制解调器组，以及其他的公用服务器放在 DMZ 区。
- 在 Intranet 网络中，DMZ 通常很小，它处于 Internet 和内部网络之间。在一般情况下，应当将 DMZ 设置成 Internet 和内部网络用户均可以访问的区域，但是应对可以访问该区域的用户数目进行严格的限制。

ⓑ 内部路由器。又称阻塞路由器，它位于内外网络与 DMZ 之间，其主要功能是保护内部网络不受 DMZ 和 Internet 的侵害。它完成屏蔽子网防火墙的大部分过滤工作，它只允许内部主机访问堡垒主机，或位于 DMZ 上的其他信息服务器。

ⓒ 外部路由器的主要功能是保护 DMZ 上的主机，它的过滤规则要求与 Internet 联系的信息均使用堡垒主机的代理服务，即它只接受来自堡垒主机上与 Internet 交换的信息流。此外，外部路由器还可以防止部分 IP 欺骗，这是由于内部路由器很难分辨出一个

自称是来自 DMZ 数据包的真伪，而外部路由器却很容易分辨出它的真伪。

ⓓ 堡垒主机。它是屏蔽子网中，外部网络与内部网络连接的主要节点，其主要功能是代理各种网络服务，例如：它可以将来自 Internet 的电子邮件转发到相应的节点，或者将发往外网的电子邮件转出；它还可以将来自外网的 FTP 访问连接到内部的匿名 FTP 服务器，并接受外来的匿名查询服务。当然，这些信息服务器都应该设置在 DMZ。在设计堡垒主机时，应遵循以下两条基本原则：

- 最简化原则　即在堡垒主机上设置的服务应当尽可能地少，对于必须设置的服务应当给予尽可能低的权限。
- 预防原则　虽然屏蔽子网防火墙非常安全，但应提醒用户做好准备，做到有备无患。这样安全系统一旦被攻破，所带来的损失就能降到最低，并能够及时修复系统。

③ 屏蔽子网防火墙的特点。

- 优点：屏蔽子网防火墙中的堡垒主机很坚固，不易被入侵者控制，万一堡垒主机被控制，入侵者仍然不能直接侵袭受到内部过滤路由器保护的内部网络。因此，这是目前安全性能最高的防火墙。
- 缺点：屏蔽子网防火墙是软硬件设备最多，费用最高，配置和管理最为复杂的一种防火墙。

15.3　代理服务技术

在前面介绍的防火墙中，大量使用了代理服务技术，从功能上看，代理服务器是代表内部网络用户与外部网络服务器进行信息交换的转换器，其硬件平台可以是网络上的任何计算机，它位于内部用户和外部服务之间，提供替代，充当服务的网关，因此，代理服务器实际上是一种软件防火墙。管理人员利用代理服务器软件来允许或禁止用户对某一服务的访问权限。代理服务常用的软件有：微软和 Netscape 公司的 Proxy Server、WinGate 和 SyGate 等。

15.3.1　代理服务

1. 使用代理服务系统的特点

(1) 优点

采用代理服务技术的优点有以下几点：

① 代理服务器可以实现内外计算机系统的隔离，从而增强了网络的安全性。

② 具有透明性是代理服务的另一个显著优点，使用代理服务后，对于用户来说仿佛是在“直接”访问 Internet，他们会认为自己直接连入了外部服务器。

③ 代理服务优化了日志服务。

④ 对于使用普通服务类型的中小型网络的管理员来说，使用代理服务器作为防火墙比使用路由器的操作、设置和管理都更为简单。

(2) 缺点

① 代理服务落后于非代理服务。由于代理服务软件广泛应用于一些老的服务,如Telnet 和 FTP 等,因此,当用户使用的服务比较新时,则很难找到合适、可靠的代理服务软件。

② 受到网络服务协议不同的影响,使得每项服务的代理需要不同的代理服务器,因此,对于服务类型复杂的网络管理员来说,选择、安装、配置和管理代理服务器将是一项庞大的工程。

③ 代理服务通常会要求对客户及过程进行分别或同时的限制,由于这些限制的存在将会导致系统性能下降。

④ 代理服务并不适合所有的网络服务。

2. 代理服务系统的工作过程

对于常规的代理服务软件,一般均包括服务器端软件和客户端软件两个部分。通过对服务器端进行简单地配置即可实现代理服务。代理服务服务器端的工作过程如下:

① 代理服务器接受来自内部客户计算机发往 Internet 的 WWW 访问请求。

② 代理服务器将自己的 IP 地址作为源地址,对客户的请求重新打包,并把打包后的请求发送给目的站点的 Web 服务器。

③ 当目的站点的 Web 服务器收到该信息包之后,就会返回一个响应给代理服务器。

④ 代理服务器收到响应,经确认无误后就转发给内部的客户计算机。

注意:代理服务器软件应当安装在 IIS 服务器上。只有这样,代理服务器的软件才会重新配置 IIS,使得该 IIS 服务器能够只接收来自内部客户机上的请求,而不会接收来自 Internet 的请求。

3. 代理服务器的类型

常见的代理服务器有应用级和回路级代理、一般与专用代理和智能型代理 3 种,受篇幅所限,不再多作介绍。

15.3.2 代理服务器的应用

如前所述,代理服务器实质上是软件防火墙,例如:其主要软件 Proxy Server 是一个防火墙软件包,通过安全配置,它可以控制 Internet 对内部网络的访问,可以允许外部网络对内部网络的有条件约束的访问,也可以完全关闭 Internet 对内网的访问。此外,它还可以提供数据缓存,利用数据缓存可以提高内外数据交换的效率。

1. 代理服务器防火墙的结构

对于普通中小型网络的管理员来说,可以使用微软的 MS Proxy Server 或者 Proxy Server 2.0 作为防火墙使用。此时,仅在 NT 服务器装上代理服务软件,而无须进行任何修改,即可将 NT 服务器当作防火墙使用。但是,应当注意代理服务器的所在位置,具体结构如图 15-5 所示。

2. 代理服务器防火墙的安装和设计的要点

① 代理服务器软件 Proxy Server 所在的计算机应当是 NT 服务器。

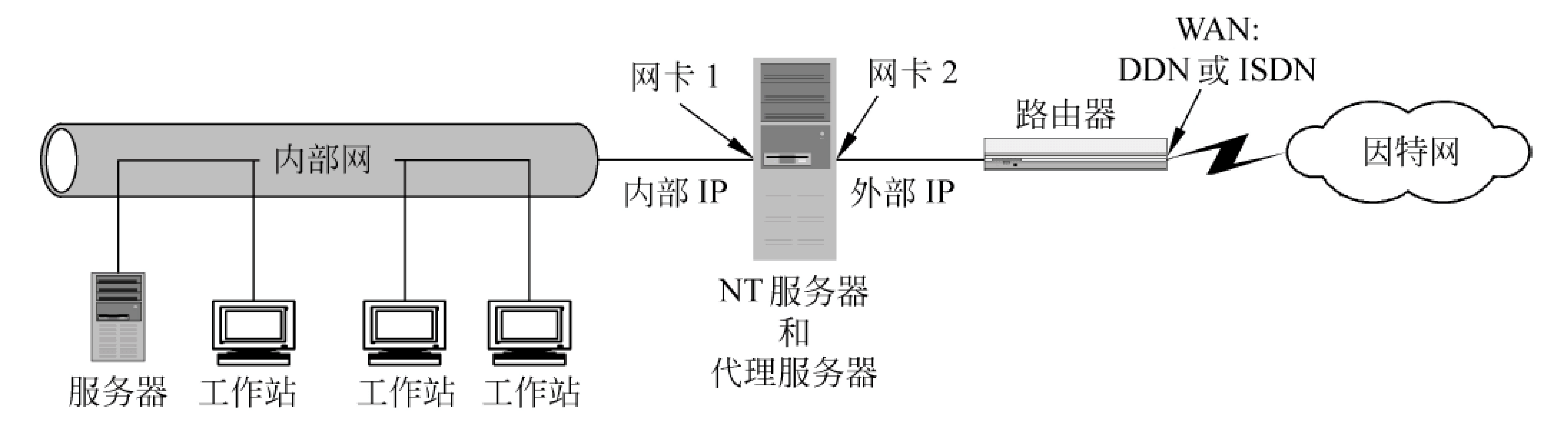


图 15-5　代理服务器作为防火墙

② 代理服务器的计算机需要安装两块网卡。

③ 1 块网卡设置和使用外部申请到的真实 IP 地址。

④ 1 块网卡设置和使用内部 IP 地址，并接入内部网络。

⑤ 按照图 15-5 所示的方式进行连接。

⑥ 在服务器端和客户端分别进行设置。

进行上述连接后，代理服务器代理内部用户进行 Internet 上的工作，起到了应用网关的作用，而它在 Internet 上隐藏了内部用户和内部网络，使得内部网络使用的 IP 地址不会直接暴露在 Internet 上，从而避免了黑客对内部系统的直接攻击，起到了防火墙的作用。此外，代理服务器还可以阻止未授权的外部用户登录并访问内部网络。过滤路由器也可以起到进一步的安全保护作用。

15.4　网络防病毒技术

15.4.1　计算机病毒和网络病毒

1. 计算机病毒和网络病毒

计算机病毒是指人为编制的、可以破坏计算机功能、计算机数据的，能够影响计算机程序或系统正常运行的一组计算机程序或指令代码。计算机病毒可以通过多种途径进行自动地复制、再生、变种、运行和传播。

网络病毒特指通过网络进行传播的计算机病毒，其传染与发作过程与单个计算机的病毒基本相同。网络病毒的感染通常从客户工作站上开始，但是它的攻击目标是网络服务器。网络服务器在病毒传播中的作用，一是感染服务器本身，造成网络瘫痪；二是使得网络服务器成为病毒传播的代理，其目的在于感染更多的计算机工作站。

2. 计算机病毒的特征

计算机病毒具有以下一些明显的特征：

① 传染性　这是判断一个程序是否是病毒的最重要的一个条件。

② 未授权性　正常的程序一般具有对用户的目的明确、可执行性和透明等特性。病毒程序具有正常程序的一切特征，它常以正常程序为宿主，并通过潜伏在正常的用户程序中而隐蔽其真正的目的。其动作的后果是未知的，也未经用户的许可。

③ 隐蔽性　病毒通常附加在正常的程序和存储介质中，其编制的目的是不让用户发现。因此，病毒常常在用户没有防范的情况下发作。

④ 潜伏性　大部分病毒在感染了其他程序或系统之后，并不立即发作，而是长期隐藏在宿主程序中，只有当病毒程序设置的特定条件满足时才发作。通常当宿主程序运行时，病毒程序也被同时启动。一旦病毒程序取得了系统的控制权，便可以在短时间内传染大量的其他程序。病毒不发作时，宿主程序还可以正常运行，当符合病毒程序所设置的条件时，病毒就会发作，达到其破坏程序和数据的根本目的。例如：CIH 病毒是一种 Windows 恶性病毒，它在符合发作时间中的时间条件时就会发作。它的发作时间分别是 4 月 26 日、6 月 26 日和每月 26 日。

⑤ 破坏性　这是病毒程序编制者的一个目的。病毒入侵系统后均会给被侵系统带来不同程度的影响，轻则降低系统的性能和工作效率，重则导致系统的彻底崩溃。例如：对于上述的 CIH 病毒，它是第一个能够直接攻击、破坏硬件的计算机病毒，是迄今为止破坏后果最为严重的病毒。它主要是感染 Windows 95/98 的可执行程序，发作时破坏计算机 Flash BIOS 芯片中的系统程序，导致主板损坏，同时破坏硬盘中的数据。

3. 网络病毒的主要来源和特征

随着 Internet 和 Intranet 网络的普及，网络病毒也越来越猖獗，许多计算机病毒程序选择了网络作为其首选的传播途径。常见的网络病毒主要采用多种传播途径：第 1，通过 FTP 下载的文件进行传播；第 2，通过用户收发的电子邮件进行传播；第 3，通过网络用户的软盘或其他活动介质进行传播。

网络病毒除了具有计算机病毒的基本特征外，还具有如下特征：

① 传染方式多样。病毒程序可以通过多种方式进行传染。例如，通过服务器和工作站的引导区、通过登录文件、通过服务器的共享目录、通过多任务加载的任务模块等多种方式进行病毒的传染。

② 传染速度快。由于网络分布距离范围广，因此，网络病毒可以在瞬间传播到分布在世界各地的计算机中。

③ 清除难度大。在单机上，清除病毒相对容易。但是，在网络中，只要有一台计算机的病毒没有清除干净，在短时间内，该病毒就会死灰复燃。

④ 破坏性强。网络病毒可以直接破坏网络中的各种资源，包括硬件、软件和数据资源。

⑤ 网络病毒还具有可激发性和潜在性等单机病毒没有的特征。

15.4.2　网络计算机病毒的防治技术

网络计算机防病毒技术是网络管理人员普遍关心和重视的问题，当然，也是一个十分棘手的问题。在实际中，除了应用网络总体的安全策略和安全技术之外，最主要的防治技术是使用网络防病毒软件。

1. 网络中常用的防病毒措施

网络防病毒措施应当从服务器和工作站两个方面分别着手。

(1) 服务器

通常采用正版的网络版防病毒软件，一般安装在文件服务器上。防病毒软件可以同时检测到服务器和工作站上的病毒。网络管理员最常采用的防病毒组织方法是：先以域的方式将多个不同功能的网络服务器组织在一起，然后，通过在域的主服务器上设置扫描方式和扫描选项的方法来防治病毒。

（2）工作站

① 无盘工作站　采用无盘工作站，或者禁止工作站上使用软驱，都可以有效地控制病毒从用户端入侵，但这样无疑会影响到用户的使用。

② 防病毒卡　使用计算机单机防病毒卡是较为方便的一种方法，并且无须设置扫描时间和扫描选项。但是，安装硬件后，一是会降低系统的性能，影响到用户的使用；二是随着病毒生命周期的缩短，防病毒卡往往处于滞后的状态，因此，目前较少采用。

③ 硬盘保护卡　使用硬盘保护卡，可以将硬盘设置为每次、每日或每周自动恢复原有的内容，也可以达到防止病毒写入的目的。硬盘保护卡为系统管理员提供了一种新的计算机系统的保护途径，目前，很多网络都使用这种方法，但是，安装硬盘保护卡之后，通常会使用户感觉到系统性能明显下降。

④ 数据保护措施　虽然采取了多种网络安全和防病毒措施，但是，网络管理员并不可以高枕无忧，因为没有任何一种防病毒的措施是万能的、可以清除一切病毒的，因此，必要的备份制度是防病毒技术的有效的辅助工具，一旦系统和数据遭到毁灭性的打击，杀灭病毒后的第一件事就是使用备份迅速恢复系统数据。

⑤ 网络防病毒软件等。

2. 网络防病毒软件的基本功能

网络防病毒软件的基本功能是对服务器或工作站进行查毒、检查、隔离和报警，发现病毒时，由网络管理员负责清除。

3. 网络防病毒软件的选择

如前所述，防病毒软件是网络服务器和工作站上常用的一种安全保护措施，选择时需要考虑的因素有：扫描速度、正确识别病毒率、误报率、技术支持水平、升级的难易程度、可管理性和报警的手段等。

4. 网络防病毒软件允许用户设置的 3 种扫描方式

网络防病毒软件允许用户设置的 3 种扫描方式如下：

① 实时扫描　该方式要求连续不断地扫描和监视系统中的文件。例如，检查从文件服务器读出或写入的每个文件是否带毒。

② 预置扫描　该方式可以在预先选择的日期和时间扫描服务器，预置扫描的频度可以是每天一次、每周一次或者是每月一次。应注意，预置的扫描时间应当是系统工作不繁忙的时间。例如，每日下班后，每周的周末等。

③ 人工扫描　该方式可以在任何时候要求扫描指定的卷、目录和文件。例如，在使用由外部复制的文件，或者是启动怀疑有毒的程序时，通常需要采用人工扫描的方法。

15.5 网络操作系统中的安全体系

为了实现网络安全特性的要求，计算机网络中常用的安全技术有：主机安全技术、身份认证技术、访问控制技术、密码技术、防火墙技术、安全审计技术和安全管理技术。

在实现网络安全系统时，通常需要先对保护的网络进行深入的分析，然后，选择和使用适合该网络的一种或几种安全技术。

每一种网络操作系统，一般是按一定的安全目标进行设计，因此，都采用了一些安全策略，并使用了一些常用的安全技术。下面以 Windows NT 为例进行简单的讨论，由于这些讨论具有普遍性，因此也适用于其他网络操作系统。

15.5.1 Windows NT 4.0 的安全概述

1. Windows NT 中的对象

对象是 NT 操作系统中的基本元素。对象可以是文件、目录、存储器、驱动器、系统程序或 Windows 中的桌面等。

2. Windows NT 4.0 的安全性设计目标

在设计 Windows NT 结构的时候，微软把目标定位于一个具有各种内在安全功能的强大而坚实的网络操作系统。

3. 使用 Windows NT 实现网络安全的策略

Windows NT 4.0 的安全机制由 3 个环节组成，即身份认证、信任确定和审计跟踪。对于每一个机构，任何操作系统的安全机制都不是自动生成的，因此，在使用 Windows NT 之前必须先制定安全策略。这些策略需要进行详细的说明，在明确了该机构对访问控制信息的保护及审核方面的具体要求之后，还需要对所制定的安全策略进行正确的配置，并实现对象的访问控制，这时才能说用 NT 构建了一个高度安全的系统。由此可见，只有将企业的安全策略和 Windows NT 底层的安全机制有机地结合起来，才能充分发挥 Windows NT 的各项安全特性。

4. Windows NT 的安全机制

微软的 Windows NT Server 提供了安全管理的功能，以及在企业级网络中实现和管理这些功能的工具。

① Windows NT 的安全子系统有：本地安全权威、安全账户管理、安全访问监督等。

② Windows NT 提供的安全机制有：登录过程控制、存取控制、存取标识和存取控制列表等。

5. Windows NT 的安全模型

Windows NT 的安全模型影响着整个操作系统，由于对象的访问必须经过一个核心区域的验证，因此，在 NT 中未经授权的申请者和用户是不能访问对象的。Windows NT 的安全模型由本地安全权限、安全账户管理器和安全参考监视器等几个主要部分组成，并且包括登录入网处理、访问控制和对象安全服务等部分。上述这些部分构成了 NT 的安

全基础，也称为安全层次。

15.5.2 Windows NT 网络安全子系统的实现

Windows NT 的安全系统应当由 3 个子系统构成：即身份识别系统、资源访问权限控制系统和安全审计系统。

满足 C2 安全等级的 NT 必须做到如下几项工作：

- 拥有对系统的非网络访问权限；
- 去除或禁止使用软盘驱动器；
- 更加严格地控制对标准系统文件的访问。

下面是 Windows NT C2 安全等级的标准特征：

- 可自由决定的访问控制　允许管理员或用户定义自己所拥有的对象的访问控制。
- 禁止对象的重用　主要表现在两个方面。第 1，当内存被一个程序释放后，不再允许对它的读访问。第 2，当对象被删除，即对象所在的磁盘空间已被重新分配时，也不允许用户对对象进行再次访问。
- 身份的确认和验证　在系统进行任何访问之前，用户必须先确认自己的身份，包括输入用户名、口令、域和组等信息的验证。
- 审核　应当创建并维护用户对对象的访问记录，并防止他人更改此记录。必须严格地规定，只有管理员才能够访问系统的审核信息。

1. Windows NT 网络的登录和身份认证机制

Windows NT 处理各种服务请求，是建立在授权许可的基础上，因此，必须先通过用户的登录和访问权限的验证，此后还需要对用户的访问权限进行限制。其验证过程分为以下几个部分：

（1）Windows NT 网络的登录机制

Windows NT 网络登录时，要求用户使用惟一的用户名和口令登录到计算机上，这种登录过程是不能关闭的，因此，称为强制性的登录。

① 登录过程。

任何一台 NT 计算机都使用 Ctrl＋Alt＋Del 3 个键的组合进行强制登录，登录过程包括对所输入的用户名和密码进行登录验证的过程。

② 登录的类型。

登录的类型分为交互登录和远程登录两种。

- 交互登录：使用本地的安全账户管理（SAM，security reference monitor）进行身份认证。当用户选择了本地 SAM，则登录时，不会发生域内的身份验证，所有的身份认证均在本地，并可以针对本地资源进行访问。
- 远程登录：当用户在一个域中的计算机上登录到一个服务器时，就会发生远程登录，也叫做“域 SAM”，此时，用户的身份认证会传递到“域”的控制器上去完成。

（2）身份识别系统

Windows NT 中的身份识别系统是网络安全系统的第一层保护，它除了进行账户和口令的检测以外，还可以由管理员限制用户的上网时间、非法使用者锁定和密码更改等。

用户账户的设置是由系统管理员来确定的，它不但是用户惟一的身份识别标志，还被分配了到域中访问资源的权限。当然，用户可以选择本地的 SAM 或域 SAM 方式进行交互式登录或者是远程登录。不同的登录方式，对资源的使用权限也不同。每一个需要使用网络的用户都应该拥有一个账户。

① 账户管理的最高权限账户—administrator 账户。

每一台 NT 计算机在安装过程中都会建立一个系统默认的 administrator 账户。该账户不能删除，但可以被更改名称。在域控制器上，此账户是一个全局账户，在其他计算机上，它只是一个本地账户。系统管理员可以使用 administrator 账户进行登录，并定义用户对资源的使用权限，进行用户账户的管理，还可以从网上任何站点进行远程登录，并行使各种管理权。使用域的 administrator 账户登录时的系统管理员可以完成以下任务：

- 可以对文件和目录的安全访问权限进行设置和控制。
- 可以对注册表进行操作。例如修改注册表。
- 可以对用户的账号进行集中管理。设置用户登录网络的账户和口令，指定登录时间，确定账户的期限及口令的使用限定等。
- 可以审计各种事件。例如用户的登录尝试设置，就是指当用户登录失败的次数超过指定的次数，系统可以将用户账号锁定。

由于，域的 administrator 账户具有很高的权限，因此，为了保证网络的安全，对该账户及其他具有同等特权的账户的账号必须采取严格的安全措施。

② 账户管理。账户管理的内容包括：用户口令控制、本地和全局账户、用户宿主目录的指定、网络登录脚本、用户强制性配置文件，以及将用户分配到默认的组等多项账户属性的操作。

(3) 账户的安全策略

建立用户账户的方法在第 8 章中已作介绍，本小节仅介绍账户安全的设置策略和步骤。

Windows NT 的默认和默认账户策略是为了便于用户使用而设计的。例如，允许用户使用空口令和选择任意长度的口令。但这些设置可以使得非法入侵者轻易地入侵网络，因此，出于安全性考虑，应当修改上述的设计策略。表 15-2 列出了建议网络管理员在各种情况下可以采取的账户策略。

注意：NT 操作系统可以自动锁定账户，管理员不能采用手动锁定账户，但是，可以进行禁止账户或解锁的操作。

(4) 账户安全策略的实施步骤

① 依次选择“开始”→“程序”→“管理工具”→“域用户管理工具”命令选项，激活如图 15-6 所示的窗口。

② 在图 15-6 所示的“域用户管理器”窗口中，选择“规则(策略)”→“账户”命令选项，即可激活如图 15-7 所示的窗口。注：有些 NT 版本中的“规则”命令显示为“策略”。

③ 在图 15-7 所示的窗口中，可以设置密码限制、账号锁定和锁定时间等，用户应当根据安全策略的需要酌情进行选择。例如，可以通过“登录失败”选项进行设定。用户允

表 15-2　推荐的 Windows NT 中的账户策略

功　　能	推荐设置	优　　点
最小口令长度	(6～8)个字符	使得所设置的口令不易被猜出
口令期限	(30～90)天	强迫用户定期更换口令，使系统更安全
口令惟一性	5 个口令	防止用户总是使用同一口令
账户锁定	5 次登录企图后锁定，30 分钟后恢复	防止黑客猜出口令的企图
最短口令的使用期限(寿命)	3 天(允许用户立即修改口令)	防止用户立即将口令改为原有的值
锁定时间	30 分钟	强迫用户等待，防止黑客猜出口令的企图
当登录时间到期时，中断远程客户与服务器的连接	应使用登录时间的限制	支持移动工作及无超时的策略
用户必须登录才能修改口令	禁止	防止用户更新已经过期的口令

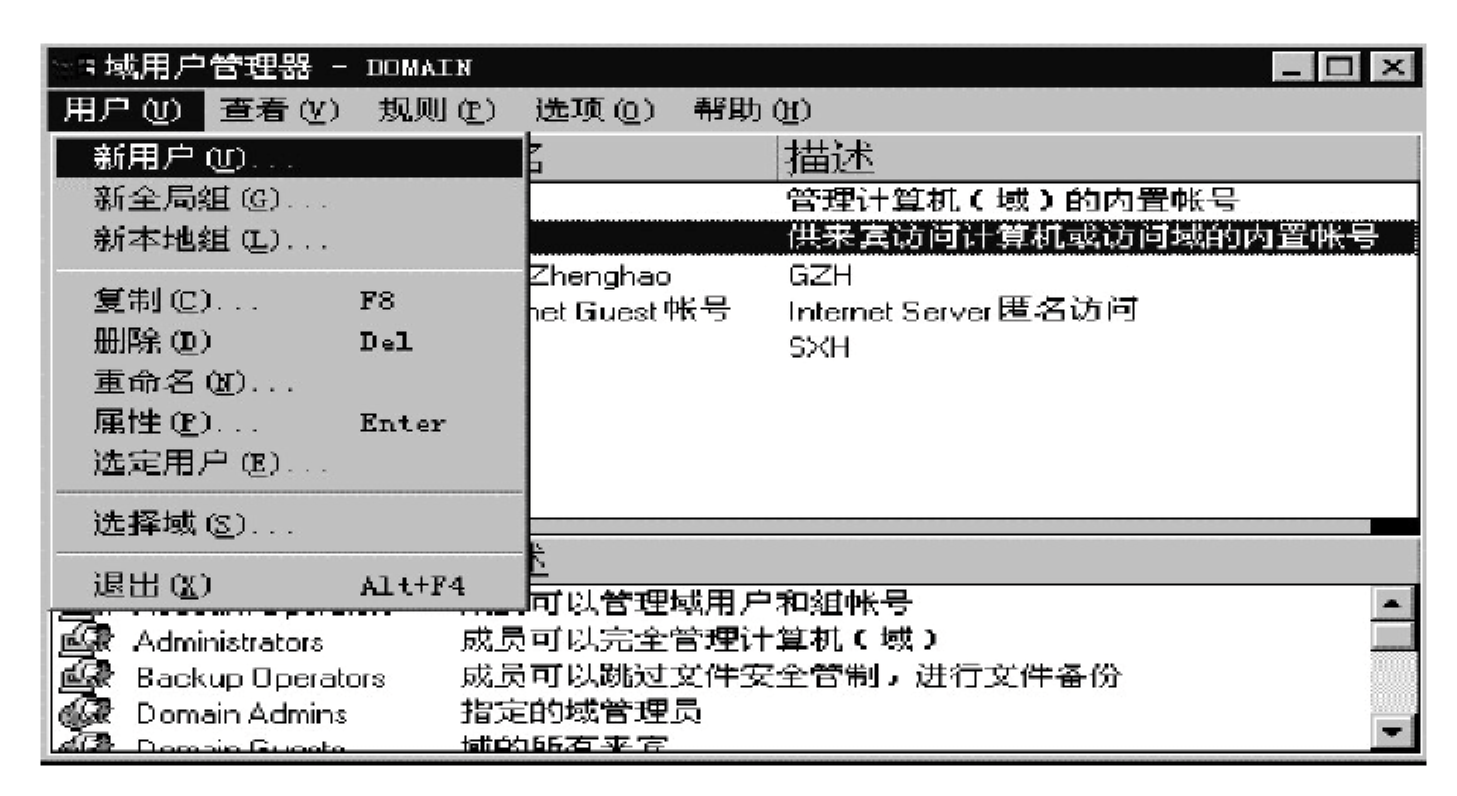


图 15-6　“域用户管理器”窗口

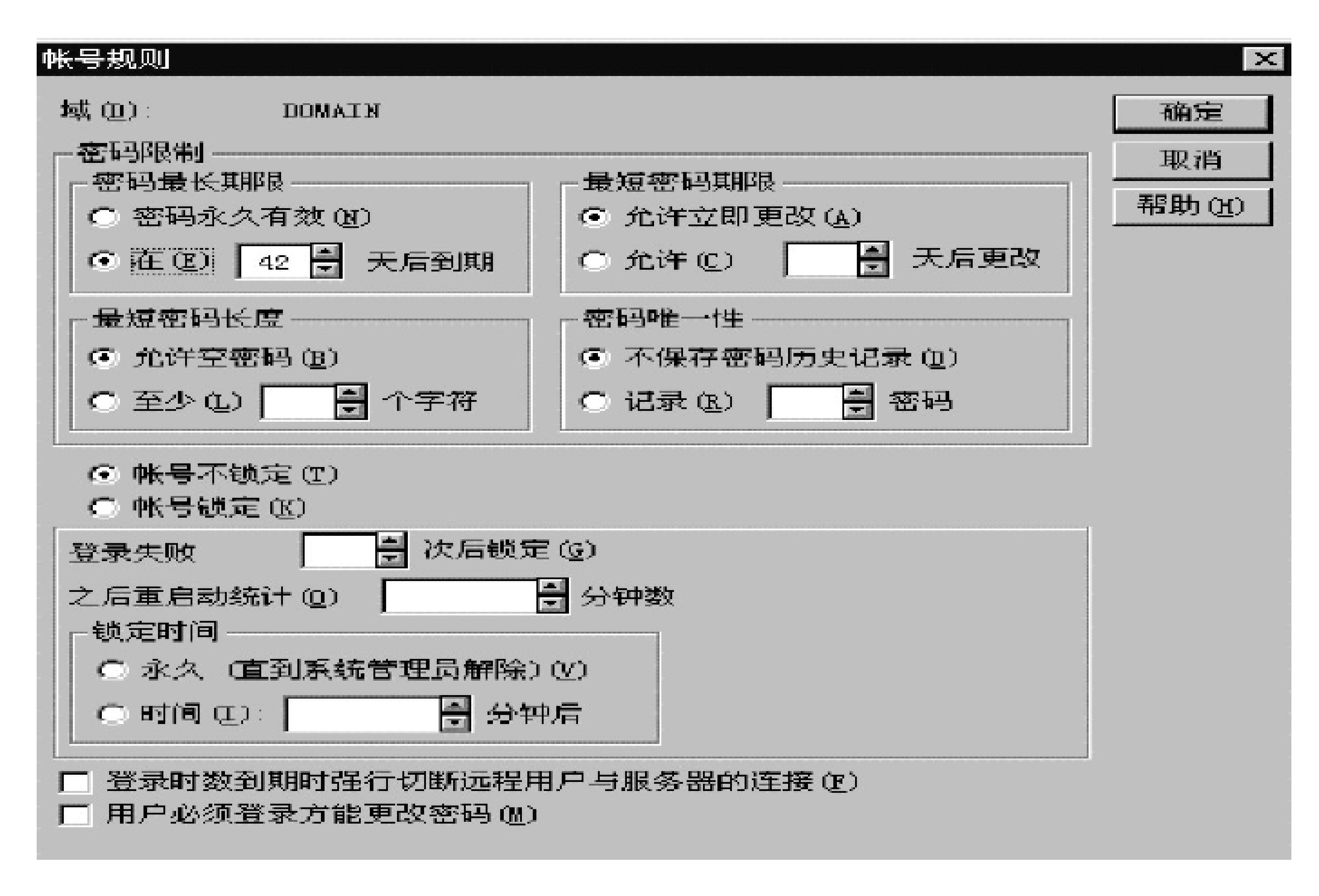


图 15-7　“域用户管理器”中的“账号规则”窗口

许的最多登录企图的次数的取值范围为 1～999。如果设定的值为 5 次，就表示用户在连续 5 次的错误登录之后，系统就会锁定该账户。

④ 对于锁定时间可以在“复位账号前锁定”选项处进行设置，通过设定用户账户，在锁定前的最大登录时间间隔，其取范围为 1～99 999 分钟。例如：如果将此时间设定为 30 分钟，就表示用户在 30 分钟之内，连续进行了允许的错误登录次数后，其账户将被自动锁定。

⑤ 在“锁定时间”处，设定对锁定账户的处理方式。如果选择了“永久”单选钮，将使得被锁定的账户在管理员解锁它们之前，保持锁定状态。如果选择了“时间”单选钮，则要求设定锁定时间，即被锁定的用户账户将在该时间之后自动解锁，从而恢复该账户的使用权。

⑥ 在图 15-7 所示的窗口中，如果选择了“账号不锁定”的单选钮，则系统对于登录失败将不进行任何的处理。注意：为了防止他人不断地登录而猜出用户的密码，最好不要选择此项，而应按照上面所介绍的方法进行必要的设置。

⑦ 为了防止用户非法访问域，每一个用户账户都要设置一个密码。Windows NT 的身份验证系统要求用户在登录 NT 网络时，提供正确的密码，否则用户的入网请求将被拒绝。设置用户密码的操作步骤如下：

- 依次选择“开始”→“程序”→“管理工具”→“域用户管理工具”命令选项，激活如图 15-6 所示的窗口。
- 在图 15-6 所示的窗口中，选择“规则（策略）”→“账户”命令选项。在激活的窗口中，选择“密码最长期限”选项，可以设置用户口令可以使用的时间，其取值范围为 1～999 天。之后，用户将被要求改变口令。为安全起见，应当要求用户经常更换他们的口令。在中等安全性的网络中，要求用户每 45～90 天更换一次口令。在高等安全性的网络中，要求用户每 14～45 天更换一次口令。当然，也可以将其设置为“密码永久有效”，为了避免密码失窃，建议尽量不要这样设置。
- “最短密码期限”选项，用来设置口令在被用户改变之前，必须要保持的时间，其取值范围为 1～999 天。值得注意的是：本项设置的时间一定要小于刚才设置的“密码最长期限”值。
- “最短密码长度”选项，用来设置口令的最小长度，由于口令越长越难被破译，因此，在中等安全性的网络中，要求用户的口令长度为 6～8 个字符。在高等安全性网络中，要求用户的口令长度为 8～14 个字符。当然，也可以设置为“允许空密码”，即允许用户不设置密码，为了保证系统的安全，建议不要这样选择和设置。

（5）Windows NT 的访问控制机制

系统的资源包括系统本身、文件、目录和打印机等各种网络共享资源以及其他对象。

在 NT Server 中，提供了控制资源存取的工具。对资源可以灵活地控制到特定的用户、多个用户、nobody、用户组或所有人等。这些控制可以由资源的所有者、系统管理员用户，以及其他被授予了资源控制权限的用户来完成。

2. 文件和目录的安全性

网络中最主要的资源就是文件和目录，因此，几乎所有操作系统的访问控制机制的安全特性都取决于文件和目录的安全性。当然，文件和目录的安全也是 Windows NT 安全模型的核心。文件和目录的安全性可以应用于单个文件、多个文件、目录或整个的目录结

构。因此，NT 的资源访问控制系统，可以确定用户对目录和文件的访问和使用的权利。它除了规定了用户所能访问的网络信息资源的目录和文件外，还可以控制用户的访问层次和范围。

(1) 通过共享许可(权限)保护网络资源

① 共享的基本概念。

共享和共享文件夹：当一个目录(文件夹)被共享时，用户就可以通过网络连接到该共享目录(文件夹)上，进而访问该文件夹中的所有文件和文件夹。因此，共享是一种开放共享资源的操作，而所开放的目录资源就被称为共享目录。

② 共享许可(权限)。

- 共享许可　在共享许可情况下，用户可以通过共享目录(文件夹)来访问网络的程序、数据和用户的宿主文件夹，但不能对目录下的文件具有单独和特定的权限。此外，当用户从本地登录访问资源时，共享目录设置的权限(许可)是无效的。
- 共享许可使用的目的　避免网络中的每个用户都安装同样的文件和目录。共享许可应用的另一个目的是将安全性运用于网络的共享资源上，例如将共享许可运用于目录上，可以实现共享目录的网络安全访问。
- FAT 分区中的共享许可　在 FAT 分区上，共享许可是使得网络资源获得安全性的惟一方法。而在 NTFS 分区上，可以通过共享许可与下面将要介绍的文件许可和目录许可对网络中的文件和目录资源进行保护。
- 共享目录许可(权限)的类型　共享目录许可的类型有 4 种，由高到低依次为：完全控制、更改、读取与拒绝访问。

③ 用户和组的共享许可。

如果管理员需要控制用户对共享目录的访问，就要给用户分配共享目录的访问权限。共享资源的权限既可以被单独地分配给用户或组，也可以被同时分配给组和用户。因此，一个用户既可以直接获得某个目录的使用权限，也可以作为组的成员获得该目录的使用权限。一般情况下，用户对某个资源的有效权限为用户权限和组权限的组合，即取用户和组权限中的较高权限。例如：如果用户对于某个目录具有了“读取”权限，同时 everyone 组被分配了该目录“完全控制”的访问权限，则由于该用户必定是 everyone 的组员，因此，用户和组的组合权限的结果是该用户对于这个目录具有“完全控制”的访问权限。

注意：“拒绝访问”权限是个例外，因为，“拒绝访问”权限总会覆盖掉其他权限，在上例中，假定该用户对该目录的权限为“拒绝访问”，而 everyone 组同样被分配了“完全控制”权限，组合结果是该用户对于此目录的访问权限为“拒绝访问”。

④ 对于用户和组分配共享许可的一般准则。

- 对被访问的资源确定允许访问的组；
- 给组分配其应具有的访问许可的类型；
- 在允许网络用户执行所需的任务的前提下，给共享资源分配最严格的权限；
- 删除新共享文件夹上的给 everyone 组分配的“完全控制”的默认权限。

注意：为了简化管理，应当尽量使用组账户进行权限设置的管理，即先把用户添加到

组中，再给需要访问该资源的组而不是单个用户分配访问权限。

⑤ 共享目录的权限(许可)的应用。

下面从网络安全的角度出发，介绍为共享目录分配许可(权限)的步骤：

ⓐ 依次选择“开始”→“程序”→“Windows NT 资源管理器”命令选项，打开 NT 中的资源管理器窗口。

ⓑ 选择拟管理的“驱动器”→“目录”，单击鼠标右键，在激活的快捷菜单中，选择“属性”选项。

ⓒ 在所选目录的“属性”窗口，选择“共享”选项卡，在该窗口中，即可对以下内容进行设置：

- “共享名”选项　应输入该目录的共享名。应注意：管理员或用户可以通过在共享名后，加一个“$”符号来创建一个隐藏的共享目录，当用户在浏览计算机时，$ 符号可以将此共享目录隐藏起来。拥有该隐藏目录使用许可的用户仍然可以使用它。
- “用户个数”选项　输入使用该资源的确定用户数目。
- “备注”选项　用于输入该共享资源的描述，通过描述能够标识共享目录的内容，该选项处可以空白。

ⓓ 在“属性”窗口中，单击“权限”按钮。在激活的窗口中，可以为用户或组分配选定目录的使用权限。此处，应先选择用户和组，再为其分配权限类型。可以选择的访问类型有“完全控制”、“读取”和“拒绝访问”等。

对于一个已共享的目录，管理员可以执行“停止该目录的共享”的操作。当然，管理员必须注意，如果停止一个用户正在使用的目录，则可能导致用户数据的丢失。因此，当需要停止目录的共享时，会出现一个对话框提醒有用户正连接到该共享目录上。

(2) 通过 NTFS 许可保护网络资源

Windows NT 操作系统一般是利用 NTFS 文件系统，而不是 FAT 文件系统来格式化硬盘的。在 NTFS 分区中可以通过共享许可和文件和目录许可两种方式实现网络资源的安全保护。由此可见，在 NTFS 分区上，除了能够实现文件和目录的共享之外，还能够在文件和目录一级实施安全措施。

① NTFS 许可(权限)。

ⓐ NTFS 许可　NTFS 许可(权限)就是只能在 NTFS 文件系统分区上使用的权限。

ⓑ 使用 NTFS 权限(许可)的目的　共享许可只能控制网络资源的访问，而不能阻止从本地登录时对硬盘的任何操作。例如，当使用共享许可的用户可以通过本地的交互式登录时，就可以从本地访问文件和目录，因此，共享许可不能保护目录和单个的文件。而 NTFS 许可(权限)不但能够控制远程登录用户的访问，还能限制本地登录用户操纵文件和目录的能力。此外，在 NTFS 中，还可以审核任何个人和组访问文件和目录事件的成败情况，即用户的权限可以分配给目录和单独的文件，所以采用 NTFS 可以提供更高的安全性。

ⓒ NTFS 许可类型　可以按文件和目录许可分为两大类，即文件许可和目录许可两类。每类 NTFS 许可又可以分别包括 NTFS 的标准许可和 NTFS 的特殊访问许可两类。

- NTFS 的标准许可(权限)　包括标准文件许可和标准目录许可两类。在大多数情况下,Windows NT 的文件系统中都使用 NTFS 标准许可。
- NTFS 的特殊访问许可(权限)　包括特殊文件访问许可和特殊目录访问许可两类。

ⓓ 文件许可　用于控制对文件的访问。文件许可又可以进一步分为标准文件许可和特殊访问文件许可两类。

- 标准文件许可的类型　拒绝访问(None)、读取(RX)、更改(RWXD)和完全控制(All)等 4 种。
- 特殊访问文件许可的类型　读取(R)、写入(W)、执行(X)、删除(D)、更改许可权(P)和获得所有权(O)等 6 种。

ⓔ 目录许可　用于控制对 NTFS 分区中各目录的访问。目录许可也可以进一步分为标准目录许可和特殊访问目录许可两类。

- 标准目录许可的类型(文件和目录的访问权利)　拒绝访问、列表(RX 和未指定)、读取(RX 和 RX)、添加(WX 和未指定)、添加与读取(RWX 和 RX)、更改(RWXD 和 RWXD)和完全控制(All)等 7 种。
- 特殊访问目录许可的类型　完全控制(All)、读取(R)、写入(W)、执行(X)、删除(D)、更改许可权(P)和获得所有权(O)等 7 种。

注意:

- 在 NTFS 分区上创建目录或文件的用户将成为该文件或目录的所有者,而所有者总是能够分配和改变资源权限的。
- NTFS 中文件的权限高于该文件存放目录所分配的权限。例如:一个用户对一个目录拥有"写入"权限,对这个目录中的某文件却只有"读取"的权限时,则用户对该文件的权限是"读取"。

对于组账户和用户账户设置、使用和管理 NTFS 权限的方法与 FAT 文件系统中共享权限(许可)的设置管理方法类似,一个用户既可以被直接分配权限,也可作为组的成员被分配权限。

在共享许可中,权限可以分配给用户和组,但共享许可只能提供有限的安全性。

在 NTFS 许可中,通过 NTFS 许可和共享许可的组合可以获得网络资源的最大程度的安全性,在这两种许可中,限制最严格的权限是用户最终得到的有效权限。

② 分配 NTFS 许可(权限)的准则。

- 移去给 Everyone 组的完全控制许可;
- 给管理员组(Administrator 组)分配完全控制许可;
- 对数据文件夹的创建组(Creator Owner 组)分配完全控制许可;
- 让用户为自己的文件分配 NTFS 许可;
- 在完成任务的前提下,为用户分配最严格的权限。

③ 应用和分配 NTFS 许可时的操作步骤。

- 在 NTFS 系统分区上的 NT Server 或 NT Workstation 上,依次选择"开始"→"程

序”→“Windows NT 资源管理器”命令选项，打开“NT 资源管理器”窗口。

- 选择拟管理的目录或文件后，单击鼠标右键，在激活的快捷菜单中，选择“属性”选项。
- 在激活的选定目录或文件的“属性”窗口中，选择“安全性”选项卡，从中选择并单击“权限”按钮。
- 在激活的窗口中，通过选择“访问类型”来为当前的组和用户分配权限。在该窗口中，所见到的是 NTFS 的标准权限。另外，从“访问类型”列表中，可以通过选择“选择性目录访问”和“选择性文件访问”选项，进一步扩充目录的访问权限。
- 选定之后，单击“添加”按钮，在激活的窗口中，可以为其他的用户和组分配所在目录或文件的 NTFS 权限。最后，单击“确定”按钮，完成对组或用户 NTFS 目录权限的分配任务。

3. 安全审核系统

审核是用来跟踪用户的活动及网络中发生的各种事件。通过审核，可以将一项指定的行为或事件记录在安全日志中。一条审核记录应该解决的问题和包含的内容：审计的对象(审计谁)、发生的行为(审什么)、实施该行为的用户(谁审计)、行为发生的时间和日期(何时审)、何时清除审计结果，以及制定合适的审计方案等。

安全审核系统也是网络操作系统中安全系统的非常重要的组成部分，它是对身份验证系统和资源访问控制系统的必要补充。安全审核系统可以保证在网络安全出现问题时，记录当前信息，为排除安全故障提供至关重要的信息。例如，Windows NT 提供了 3 个事务审核与跟踪的系统，即安全日志、系统日志和应用程序日志。

(1) 审核策略的拟定与实施

在拟定和实现一份审核策略时，应考虑和注意如下因素：

① 明确所审核的类型和事件。常见的审计类型有 3 类：系统审计、应用程序审计和用户自行配置的安全性审计等。例如，用户的登录及登录退出、文件或目录的使用、关闭和重新启动 Windows NT Server、用户和组的改变以及安全规则的改变等。

② 明确审核的是事件的成功还是失败的记录。

- 跟踪事件的成功记录能了解文件和打印机的访问频率，从而有助于进行资源规划。
- 跟踪事件的失败记录将对非法入侵发出警报。
- 在中等和高等安全的网络中，应该跟踪用户登录成功和失败的记录，及资源的使用情况。

③ 决定是否需要跟踪事态的发展。如果需要，应该有计划地将安全日志进行存档或清除。

④ 确定审核策略设置的位置。审核策略的实现位置是基于本机的。例如：对于审核发生在“主域控制器”上的事件，如用户登录和改变用户账户等，必须在“主域控制器”上设置审核策略。而要想审核其他计算机的事件，如访问一个成员服务器上的文件，就要在成员服务器上设置审核事件。

⑤ 审核的实施者。只有域的管理员(administrator)能够设置域控制器上的文件、目

录和打印机的审核。对于非域控制器的计算机，只有本机的管理员组（administrator 组）的成员才能设置审核。当审核设置好之后，管理员组的成员都可以查看并保存安全日志，完成其他的管理任务。

⑥ 对于文件和目录的审核，只能在 NTFS 分区上完成。

注意：设置太多的审核任务将会加大系统的负荷。如果服务器已经很繁忙，我们应该将审核任务减到最少。

（2）安全审核系统的设置

在 NT 网络中审核系统的设置可以分成两个主要部分。其一，设置选定计算机中需要审核的事件。其二，设置其他要审核对象的审核事件。例如文件、目录和打印机等对象的审核事件等。

在 PDC 上可以设置域的审计事件。设置 PDC 计算机中需要审核事件的步骤如下：

① 选择“开始”→“程序(P)”→“管理工具(公用)”→“域用户管理器”激活图 15-6 所示的“域用户管理器”窗口。

② 在图 15-6 所示窗口，选择菜单项“规则(P)”，选择其中的“审核(D)”选项，激活如图 15-8 所示的“审核规则”窗口。

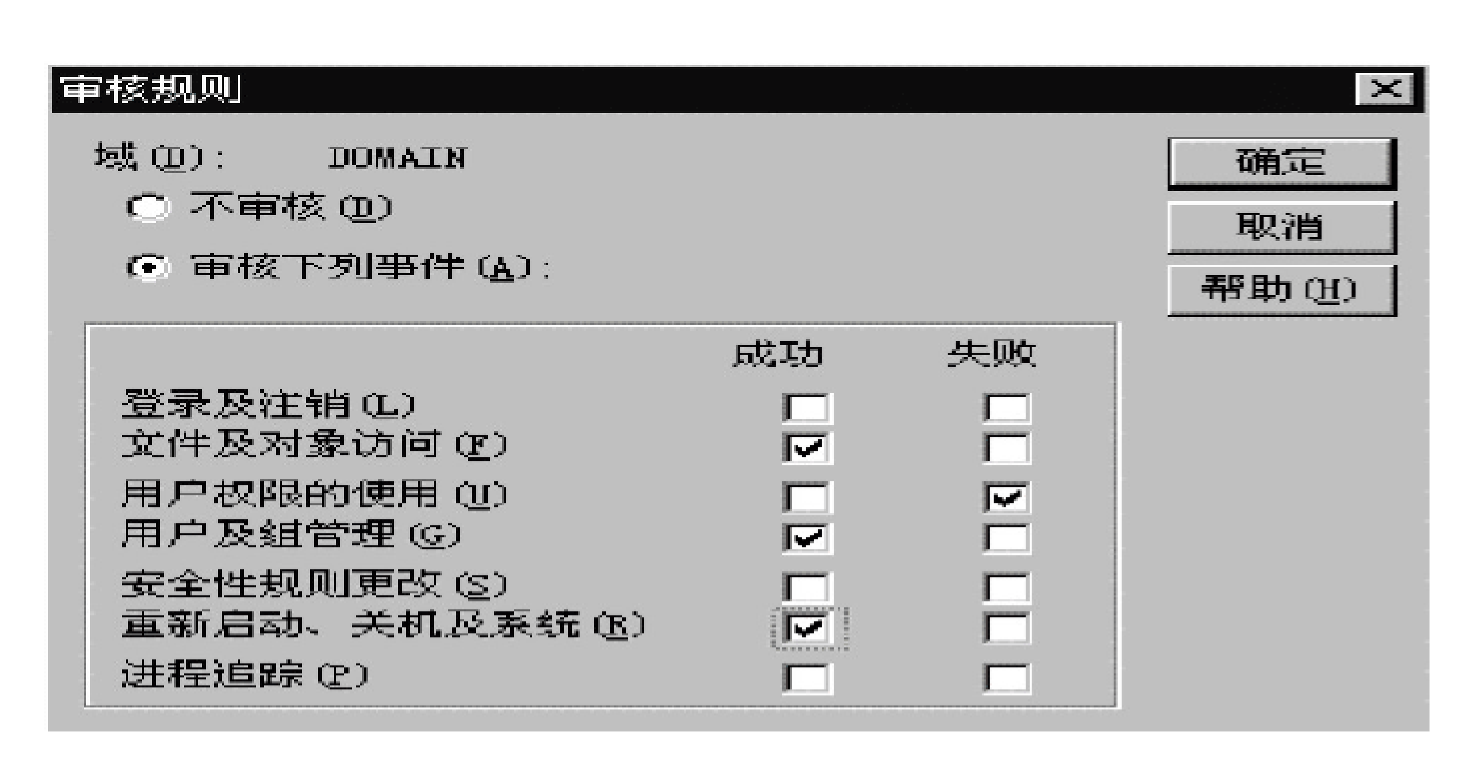


图 15-8　“域用户管理器”中的“审核规则”窗口

③ 在图 15-8 所示的窗口中，管理员既可以审核成功的操作，也可审核失败的操作。当选择某安全事件之后，可以将复选框打上“√”。

④ 系统可以审核的事件说明如下：

- 登录及注销　指用户的登录或登录退出。通过网络与一台服务器建立连接或断开连接。
- 文件及对象访问　指设置了用户访问目录、文件和打印机的审核。
- 用户权限的使用　指用户使用了某种权力（有关登录或登录退出的权力除外）。
- 用户及组管理　指创建、删除或重新使用一个用户账户或组，更改用户口令，重新命名、禁止或重新使用一个用户账户。
- 安全性规则（策略）更改　指更改用户权力，审核规则或信任关系。
- 重新启动、关机及系统　指用户重新启动或关闭计算机，或者是影响到系统安全或安全日志的事件，例如安全日志已经满了。
- 进程追踪　指对各种事件的详细跟踪记录信息，例如程序的启动。

⑤ 完成上述的设置之后，应当进一步设置其他要审核对象的审核事件。例如，可选择或指定的其他可审核的对象有文件、目录和打印机等。

(3) 使用事件查看器查看审计的数据

安全审核系统将审核的结果保存在系统的各种日志中，管理员通过事件查看器可以查看系统的日志。事件查看器可以提供出错信息、警告信息，以及执行某项任务的成功或者失败等内容的具体信息。这些信息存放在以下 3 类日志内：

① 系统日志　包括系统产生出错信息、警告信息以及提示信息。这是由 Windows NT 预先设定好的。

② 安全日志　包括设置审核事件成功或是失败的信息。这些事件都是在审核规则中设定的。

③ 应用日志　包括应用程序产生的出错信息，警告信息以及提示信息。这是由程序开发者事先设定好的。

习题

(1) 什么是计算机安全？它包含哪些主要内容？

(2) 破坏计算机安全的途径有几种？

(3) 保护计算机安全的常用措施有哪几种？

(4) 可能受到威胁的网络资源有哪些？有意危害 Internet 安全的是哪 3 种人？

(5) 什么是网络安全？网络安全的主要内容有哪些？

(6) 网络安全体系所要求的 6 类基本安全服务是什么？

(7) 网络安全的评估标准是什么？其中 D、C1 和 C2 级别具有什么特点？

(8) 请说明 NT Server 上实现 C2 安全等级时，应当做到的有哪些？

(9) 计算机安全保护的目的是什么？保护计算机安全的措施有几个？

(10) 计算机网络安全的目标有哪几个？

(11) 网络中通常采用的安全机制有哪几种？什么是数据加密？

(12) 网络安全保护的主要策略有哪几条？什么是最小特权(授权)原则？应如何应用到系统的账户管理中？

(13) 常用的网络安全技术有哪几种？

(14) 什么是防火墙？防火墙的基本结构是怎样的？有哪些主要部分？

(15) 防火墙的基本功能有哪些？在组建 Intranet 时为什么要设置防火墙？使用防火墙的优点如何？缺点又如何？

(16) 防火墙的基本类型有哪几类？各有什么特点？适用哪些场合？

(17) 请解释防火墙的有关术语：①防火墙 ②主机 ③堡垒主机 ④双宿主主机⑤数据包 ⑥周边网络(非军事区 DMZ)⑦代理服务器。

(18) 实用的防火墙有哪几种？画出它们的应用结构图，并说明各类防火墙的工作原理和结构特点。

(19) 画出包过滤型防火墙的结构图，并说明该防火墙的工作原理、设计要点和应用特点。

(20) 请说明使用代理服务器作为防火墙时的设计要点，并画出网络结构示意图。

(21) 网络安全保护策略有哪几种？

(22) 计算机病毒和网络病毒的主要特征？网络病毒的主要来源是什么？

(23) 网络服务器在网络病毒事件中的两个作用是什么？

(24) 网络防病毒软件的基本功能有哪些？又应如何选择网络防病毒软件？

(25) 网络防病毒软件允许用户设置的 3 种扫描方式是什么？如何规定的？扫描时间又是如何考虑的？

(26) 网络工作站防病毒方法有几种？各有什么特点？

(27) 从网络安全的角度看，网络用户的责任是什么？网络管理员的责任是什么？

(28) Windows NT 网络安全模型由几个部分组成？它的安全性设计目标又是什么？

(29) 在 Windows NT 的登录过程中包括哪两类登录方式？

(30) 基于 FAT 和 NTFS 文件系统中 Windows NT 网络资源的保护方式有什么不同？

(31) 对于用户和组分配共享目录权限的一般准则是什么？

(32) 共享权限(许可)的特点是什么？在实施目录共享许可时，可选择的类型有几种？

(33) 什么是 NTFS 权限？NTFS 权限(许可)的类型有哪些？

(34) 应当如何分配 NTFS 权限？其目录和文件权限是如何组合的？

(35) Windows NT 网络的身份识别系统包括什么内容？

(36) 在拟定审核规则方案时，应解决的主要问题是什么？应考虑因素有哪些？

(37) 设置审核系统时，分成哪两个主要部分？

(38) 事件查看器有什么用？安全日志的作用是什么？包含哪些内容？

(39) 在哪一台计算机上可以设置对域登录的审核？

(40) 如果需要对一台运行 NT Workstation 的计算机进行某个目录的审核，应该在哪一台计算机上进行审核策略的设置？谁有权设置审核策略？谁有权管理审核策略？

(41) 计算机系统可以审核的事件有哪些？对于审核目录来说，可以审核的事件有哪些？

实训题目

1. 在小型网络或部门网络的计算机中使用代理服务器软件接入 Internet。

2. 设计、分配和使用 FAT 系统下共享目录的权限。

① 试为该共享目录的不同级别的访问者分配不同的权限。

② 试为某共享目录创建一个隐藏的共享名，并通过网络访问该共享目录。

3. 设计和分配用户和组在 NTFS 系统下对单个目录或文件的权限，并得出该组合的

正确结论。

① 试在 NTFS 分区上为文件或目录分配 NTFS 的标准许可，并将该许可赋予组或用户。

② 试在 NTFS 分区上为目录和该目录下的某个文件分配不同的权限，并得出该组合的正确结论。

4. 资源和事件的审核——设计一份有效而可靠的审核策略。执行该审核计划，并使用事件查看器查看审核的结果。例如：确定资源管理器中的文件和目录的审核，或者是打印机的审核。



网络管理员的职责综述

在介绍了前面各章的内容之后，本章通过一个综合案例的实现，概括网络管理员在日常工作中的主要职责和具体内容。本章着重总结与网络管理相关的实际工作重点，并进一步明确网络管理员的工作目标和基本职责。

主要内容：

- 网络管理员的责任与应遵循的准则；
- 网络管理中的工作重点；
- 小型办公网络的管理案例；
- 网络的维护与故障处理；
- 网络管理员职责综述。

16.1 网络管理员责任概述

随着网络规模的扩大，故障的数量和故障对网络的影响程度均会随之增加，网络管理员的工作范围和复杂程度也相应地不断增长。为了完成管理任务，网络管理员只有清楚地知道有关网络的大量信息，才能对其实施有效的管理。如果不是网络管理员自己设计和建设的网络，则首先应当了解所管辖计算机网络的组成方法和有关信息，并进一步明确所担负的责任和网络管理的准则。

16.1.1 网络管理员的责任

建立计算机网络的基本目的是实现资源共享和满足网络通信的需求，为了实现这一目标，在制定网络建设的规划和设计时，网络管理者必须根据用户的需求，确定网络的总体布局。当然，这个规划设计可以是全新的，也可以是一个现有网络的扩建或改建的规划和设计。在规划设计完成之后，网络管理者还需要完成建设、扩建、维护、优化及故障检修等工作。网络管理员在网络系统规划与设计和后期管理、维护工作中的主要责任如下：

1. 选择合适技术实现网络设计

网络管理员应当根据网络的规划设计，选择建设网络需要的软件、硬件，以及网络互

联的部件。例如，确定局域网（LAN）与广域网（WAN）互联时使用的技术，确定互联设备和互联软件，在实现这个目标时，必须解决上述两种网络在传输速率、网络结构、软件和硬件之间的巨大差异。

2. 扩展网络

网络管理员经常会遇到改扩建网络的要求。如用户根据自己当前的需要，要求改变网络的设计，扩展已建成的网络。这时网络管理员就应当针对现存网络进行重新设计，提出适当的网络扩展和连接方案。例如，将原有的100Mb/s共享式以太网扩展或改建为100Mb/s交换式以太网或千兆以太网。

3. 维护网络

不管网络建设和验收的步骤多么细致，毫无疑问地说，网络管理员必然还是经常会面临网络的维护工作。例如，当网络需要重新划分子网时，网络设备的软件必须重新设定。又如网络配件的更新也是经常遇到的。

4. 提高网络的性能

每一个网络有着不同数量、不同类型的设备，少则十几台，多则上千台。每个设备都有自己的运行特性，它们必须在一起协调地工作，这就需要网络管理员通过长期和仔细的调整，才能使得它们处于良好的运行状态。例如，当每一种新产品或技术引入时，很可能会影响到网络的性能。如某小区宽带网络，为了解决用户的专有带宽问题，专门购买了第3层的交换机，投入后，用户端的操作却总出现问题。网络管理员只有仔细地研究，才能知道该产品的哪些参数是必须设置的，哪些是与目前网络管理无关的，这样方可获得最佳的系统性能。

5. 检修网络，处理网络故障

正像没有不生病的人一样，也没有无故障的网络。无论网络设计和管理得如何好，网络总会出现故障。因此，必须制定出网络故障处理的计划，并落实到每一个人，这样才能使网络故障得以及时处理。

16.1.2 网络管理中的工作重点

具体的网络维护与管理工作与外科医生的工作有些类似，正像外科主治医生在施行一例肾脏移植手术之前，必须具有丰富的理论支持、多年的临床经验、本次手术的精心准备以及先进的医疗设备一样，网络管理的专门人才在管理一个大规模的网络之前，也必须具有坚实的专业理论的支持和数年的实际工作经验。他们在解决大型网络的复杂故障时，往往会熟练地借助于网络的语言——“协议”，并能通过复杂而昂贵的管理和诊断工具软件，迅速地解决问题。然而，对于大多数的网络故障和管理而言，并不是都需要具有很高技术的专业人员来解决问题。例如，当一个惠普公司的网络打印机不能工作时，作为网络的日常管理员，大可不必招来该公司的专职网络技术人员进行诊断，因为，可能只是简单的打印纸张的阻塞、硒鼓的损坏，或者是该网络设备的配置出现了故障，完全可以自己判断解决。

因此，在实施网络管理系统之前，应当根据自己所管理的对象来考虑具体的工作内容和网络管理中的重点与难点。例如，对于一个大规模的校园网和一个小型办公室的网络

来说，管理工作的内容、重点和难点的差别就很大。

1. 日常网络管理工作中的工作重点

下面将简述网络管理员在日常网络管理工作中的具体工作重点。

（1）合理的流量控制

网络管理首先必须解决的问题是数据通信网络中的流量控制问题。因此，网络管理员应当清楚网络的规划与设计，明确网络中的瓶颈所在。

（2）正确选择路由策略

在大规模的网络中，应当确定和管理好网络路由的选择策略，使之具有正确、平稳、公平和简单的特点，并能够适应网络的规模、网络的拓扑结构和网络数据流量的变化。对于那些中小规模的网络管理员来说，应当在网络施工之前，通过选择合适的网络系统结构和设备来确保网络不会出现瓶颈。

（3）明确和落实各级网络管理员的分工

对大型网络来说，网络管理员可能是分层管理的，因此，各级网络管理员的管理与培训措施的确定和实施是不可缺少的，因为只有这样，才能确保网络的平稳运行，以便在出现故障时，能够及时恢复与处理；而对于小规模网络的管理员来说，往往既是网络的设计者，也是网络的实施和管理者，因此，管理和培训措施就较为简单，主要是明确分工，保证网络的正常运行，出了故障有人处理。

（4）必要的网络安全防护措施

引入必要的安全机制和数据保护机制，以保护系统安全运行和网络资源的保密性、完整性、可用性、真实性和可控性。对于大规模网络来说，往往会综合使用多种安全措施，例如，同时使用数据保护技术、防火墙技术、身份认证机制、网络资源的访问控制机制与安全审计机制等多项安全措施；而对于简单的办公室网络，可能仅仅需要使用数据备份、防病毒技术和软件防火墙等较为简单而又行之有效的安全措施。

（5）网络故障的准确诊断

网络的故障诊断系统应能够准确、快速地确定故障的性质和位置。对于较大规模的网络，可能需要借助于价格不菲的网络诊断工具；而对于小型网络来说，往往是网络管理员通过网络操作系统中的一些命令，凭借自身的诊断能力来完成故障的诊断、定位和处理的。

（6）适合的网络计费系统

对于商业型网络来说，网络费用的计算是必不可少的，其网络的计费系统应当能够对用户使用的网络资源进行计算，并估算出应支付的费用；而对于大多数普通网络来说，往往没有此功能。

2. 网络常见故障的处理

目前，计算机网络广泛地应用于各行各业，这是可喜的一面，但也应该看到，层出不穷的网络故障为日常网络维护工作带来了许多麻烦，对工作也造成了很大影响。因此，了解和掌握网络常见故障的处理方法是网络管理员不可缺少的一课。

在网络维护工作中，通常遇到的网络故障，处理起来都不是太复杂，实际上判断故障是其关键所在。下面就常见故障的类型及其处理方法作简要介绍。

（1）服务器故障

当服务器出现故障时，所有的工作站都将不能正常工作，就服务器而言，其故障表现在以下几个方面：

① 服务器的引导分区故障　此故障表现在服务器不能正常引导，表明分区引导系统有故障。例如，DOS 引导分区出现故障时，可以使用一张干净的系统引导磁盘引导系统，查看引导分区的文件是否存在或损坏。如果表明只是引导文件被损，则可以先杀毒，然后重传系统分区文件。

② 操作系统启动故障　可以使用紧急修复磁盘修复系统。例如，在 NT 系统中，可以使用 3 张系统安装引导磁盘和紧急修复磁盘修复系统。

③ 服务器连通性故障　如果原来服务器工作正常，因此，故障可能是出现在服务器的网卡、介质连接器上。此时，可以检查网卡与主板的接触，或者是介质连接器的接触是否良好。如果检查不出问题，则可使用网卡替代法来判断原有网卡是否出现故障。

当然，对于不同操作系统的修复方法和手段各不相同，这还需要管理员在长期的维护工作中，不断总结和提高。对于 NT 系统中的恢复方法，用户可以参见本书的有关章节。

（2）传输介质和连接器的故障

在网络维护工作中，传输介质的故障是经常发生的，其故障主要表现为以下几类：

① 网线故障　对于总线式网络，经常表现在网线的电阻不正常，例如，对 10Base-2 网络而言，其正常的内外线电阻应当是 25 欧姆。若测出的电阻值为无穷大，则表明网线断路；若测出的电阻值为 0，则表明网线短路。判断之后，即可排除故障。对于 10Base-T 或 100Base-T 星型网络，网线故障的处理很简单，因为，每段网线只影响一个节点，因此，可以使用网线替代法进行检测，哪段有故障就处理哪段。

② 网线连接器故障　网线连接器俗称网络“接头”，此种故障的现象是个别工作站不能正常启动和连接，其他工作站工作正常。例如，对于 10Base-2 总线网络而言，问题多出现在 BNC 头或 BNC-T 型头接触不良，更换不良接头即可解决问题。对于 10Base-T 星型网络而言，更换掉有问题的 RJ-45 接头即可。

（3）工作站的故障

对工作站而言，其故障多表现在以下几个方面：

① 单台计算机工作站无法登录　由于原先工作站能够正常工作，因此，故障可能是出现在工作站的网卡、介质连接器、系统引导分区上，此时的处理办法与服务器的类似。

② 整个网络登录异常　可能是某个网卡的短路而引发的整个网络故障，处理方法是依次断开每个工作站的网线，如果断开后网络恢复正常，则更换有故障的网卡。

③ 个别工作站登录缓慢　一般是由于登录缓慢工作站的网卡的质量变坏或是接触不良而引起的，可对这些工作站分别作处理。

上述的故障处理方法适用于大部分的场合，但是，引起网络故障的原因可能是错综复杂的，因此，对网络故障的判断和解决办法不是一朝一夕就能解决问题的。只有经过长期的不断的实践、摸索和总结，才能成为一名合格的网络管理员。

16.2 小型办公室网络的组建和管理案例

随着网络的普及，网络管理员的责任问题越来越突出，有时候，网络上的用户不得不花费大量的时间，去学习与其本身工作无关的“网络使用”技术，因此，在现代化网络中，进行网络管理工作的人员首先必须明确自己的基本工作目标是使网络用户应该能够自动地获得网络给他们带来的种种好处，而不必时刻记住自己工作在网络环境中；其次，网络管理的最终目标应当是网络管理员自己也不必为担负的网络管理工作而担心。为了实现上述的现代化网络管理的目标，可能还要走很长一段路。目前，作为网络管理员的最基本的任务，就是在企业内部局域网或 Intranet 建立好以后，能够运用网络管理软件或者是自身的经验，来保证网络的可靠和安全运行。

为了保证网络的正常运行，网络管理员应该明确自己应该完成的主要工作。网络管理员最基本的职责就是将属于本企业的 Intranet 网络建立起来，在以后的工作中确保网络正常、安全、可靠运行，并能够及时排除网络故障；同时为网络用户提供必要的支持，对网络系统和网络资源的安全管理也负有重要的责任。

网络的规模有大有小，小到家庭中的两台计算机组建的“家庭网络”，大到一个跨国公司组建的跨越洲际的大型网络。无论大与小，他们之间都有一些共同的地方。千里之行始于足下，在此以一个小公司的网络建设为例，来说明和总结一下网络中的基本组件、网络的设计、组建和网络管理等基础管理工作。

1. 分析案例的现有条件及要求，确定网络系统结构

该小型办公室具有 5 台左右的计算机，可能会发展到 10 台；办公室现有一条 ISDN 电话线、一部传真机和一个 modem，要求提供共享 Internet 的访问，以及共享一些内部资源，如程序文件、打印设备和刻录机等。

作为小型的公司，应当兼顾未来的发展，10/100Base-T 型以太网可以说是较好的选择。这种网络结构十分适合那些需要不断增长的网络，此外，它还具有传输速率较高、可靠性好、成本低、易于安装和维护、扩展方便等特点。因此根据此案例的情况，可以确定其网络系统结构如图 16-1 所示。

2. 选择并确定主要部件

根据系统的结构图，确定需要增加的主要部件如下：

① 选择 16 口的 100/10Mb/s 桌面或工作组交换机作为网络的连接设备，连接各服务器和计算机，各服务器应接在交换机的 100 Mb/s 端口，以确保其带宽不至于成为网络的瓶颈，高速工作站也可以接在交换机的 100Mb/s 端口。如果资金紧张，也可以购买 8 口的 10/100Mb/s 自适应集线器。其他计算机通过内部的网卡连接到交换机或集线器上。

② 选择购买小型 ISDN 路由器一台，作为局域网与 Internet 的连接设备，也可以兼作包过滤路由器，起安全保护作用。如果资金紧张，也可以依图 16-1 的连接方式连接，即只购买 ISDN 卡（200 元左右）和另一块网卡。

③ 网卡　服务器网卡2块（100Mb/s、RJ45口、PCI卡）；工作站网卡（10Mb/s、RJ45口、PCI卡），根据需要购买若干块。

④ 网线　在图16-1中的各段电缆线可以采用5类UTP（非屏蔽双绞线），两头采用RJ-45水晶头。

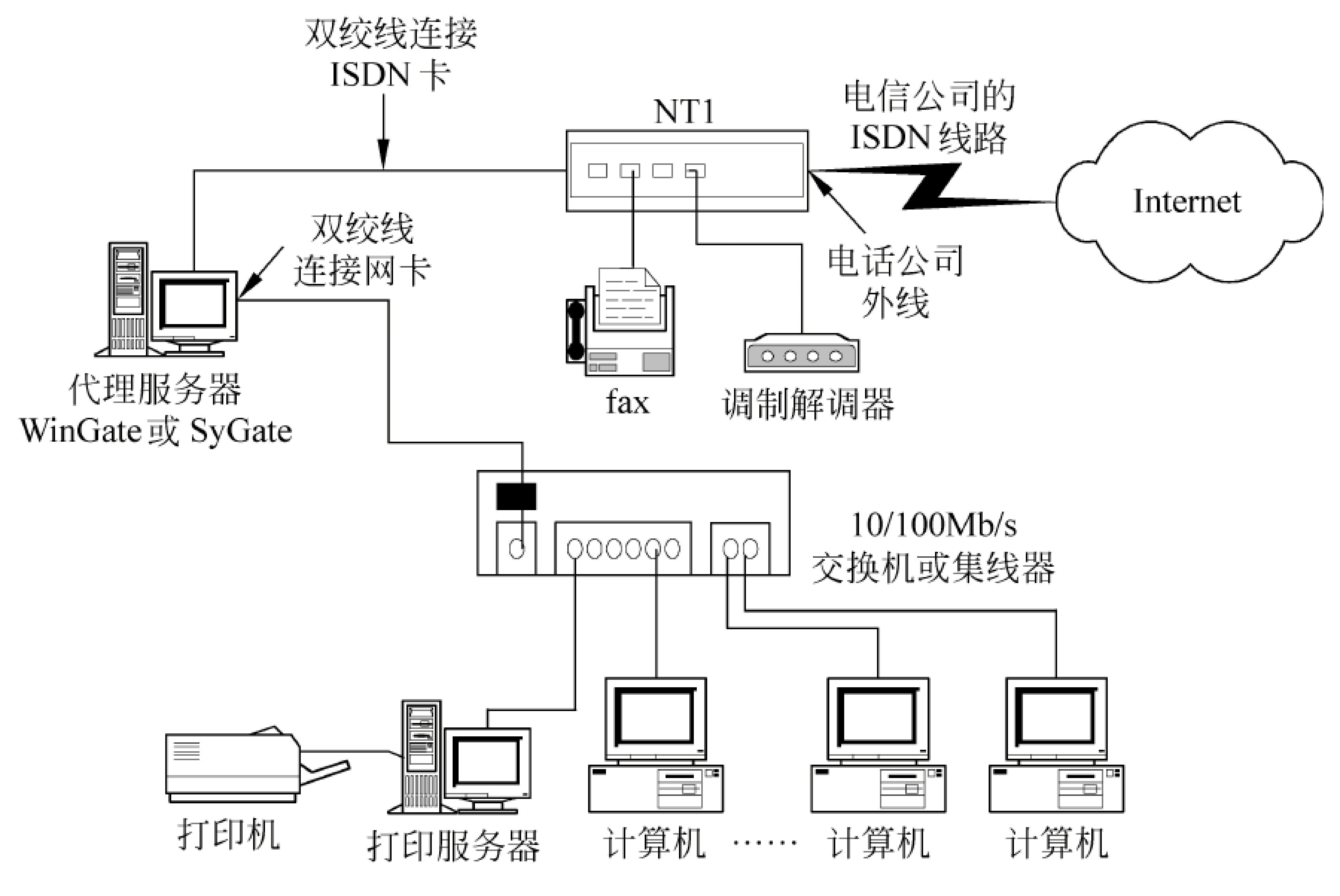


图16-1　小型办公网络系统结构图

3. 网络布线设计

设计和安排好各计算机和打印机的位置，由于需要实现Internet共享，因此应当确保一台作为网络代理服务器的计算机靠近ISDN的终端设备NT1。

当所有的计算机都在同一房间内时，可以将5类UTP电缆线放置在计算机的后部。如果计算机不在同一房间内，需要将网线安置在墙体内部或PVC槽内，或者需要将电缆线穿过门窗或墙体时，则应当聘请专业施工人员进行综合布线。

10/100Base-T的网络使用不超过100m的双绞线将每一台计算机或网络设备连接到交换机或集线器上。因此，应当注意核心设备集线器的摆放位置。

在制作连接用的网线之前，需要认识的部件有RJ-45连接器、网卡（RJ-45接口）、ISDN卡和非屏蔽双绞线。

① RJ-45连接器，俗称水晶头，用于连接UTP，其结构如图16-2所示。共有8个引脚，一般只使用了第1、2、3、6号引脚，其定义与网卡不相同。各引脚的意义如下：

- 引脚1　接收（Rx+）；
- 引脚2　接收（Rx−）；
- 引脚3　发送（Tx+）；
- 引脚6　发送（Tx−）。

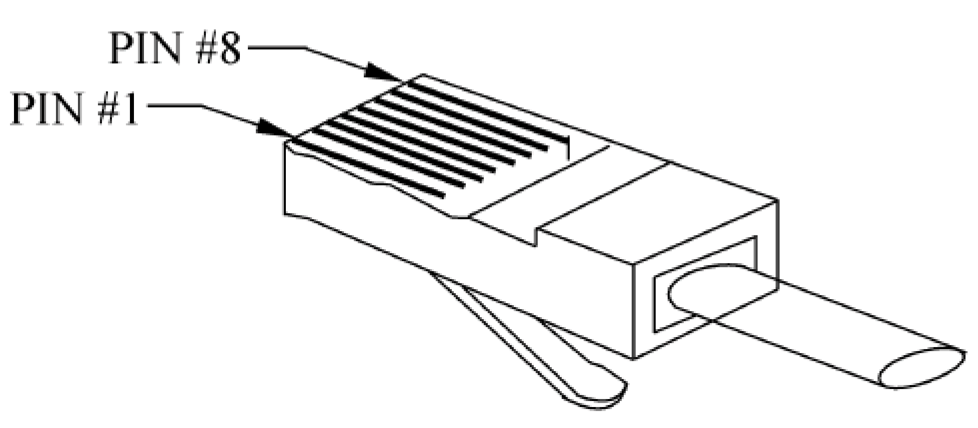


图16-2　RJ-45水晶接头

② 网卡上的RJ-45接口也有8个引脚，一般也只使用第1、2、3、6号引脚，其余的没有使用，各引脚的定义如下所述：

- 引脚 1　发送(Tx+)；
- 引脚 2　发送(Tx－)；
- 引脚 3　接收(Rx+)；
- 引脚 6　接收(Rx－)。

③ 组建 10Base-T 网络所需的工具如下：

- 驳线钳　RJ-45 专用剥线/压线钳，用于接驳水晶头。
- 网线测试仪(测线器)或万用表　当网线两头接好后，应进行测试，以确定线路是否通畅。

④ 制线的方法如下所述：

- 准备好长短合适的双绞线，用 RJ-45 专用剥线/压线钳，剥出 1.5～2cm 长的双绞线。
- 将剥好的双绞线，按表 16-1 或表 16-2 排好顺序，例如，按 TIA/EIA 568B 标准的线序排列。
- 用 RJ-45 专用剥线/压线钳剪齐，留出 1cm 左右长的双绞线头。
- 将排好顺序的双绞线插入 RJ-45 接头，参见图 16-2。应当注意，所有 8 根细线应顶到 RJ-45 接头的顶部(从顶部能够看到 8 种颜色)，同时应当将外包皮也置入 RJ-45 接头之内，最后，再用 RJ-45 专用剥线/压线钳将接头压紧，并确定无松动现象。
- 将另一个 RJ-45 接头以同样方式制作到双绞线的另一端。
- 使用 RJ-45 测试仪或者万用表依次测试 RJ-45 接头上的每一路线，必须保证全部接通。

表 16-1　10 /100 Base-T 双绞线、RJ-45 接口连接顺序表(TIA/EIA 568A)

	1	2	3	4	5	6	7	8
工作站(集线器)	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕
工作站(集线器)	绿白	绿	橙白	蓝	蓝白	橙	棕白	棕

表 16-2　10 /100 Base-T 双绞线、RJ-45 接口连接顺序表(TIA/EIA 568B)

	1	2	3	4	5	6	7	8
工作站/服务器	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕
集线器	橙白	橙	绿白	蓝	蓝白	绿	棕白	棕

⑤ 标准线和交叉线的制作与使用。连入 10/100Base-T 网络的每个节点需要一块支持 RJ-45 接口的 10Mb/s 以太网网卡，或便携机网卡。网卡与双绞线电缆上的 RJ-45 型接头直接连接。在连接网络设备时，应注意学会以下两种线的制作与使用。

- 标准线　又称直通线，制线时两头一致，通常两头均按 TIA/EIA 568B 的标准制作。标准线主要用于 hub/交换机/路由器与计算机节点上网卡的连接。当然，也可以两头均按 TIA/EIA 568A 的标准制作，见表 16-2。
- 交叉线　又称跳阶线，两头不一致，一头按 TIA/EIA 568B 标准制作；另一头按

TIA/EIA 568A 标准制作，见表 16-1 和表 16-2。交叉线主要用于双机互连(不通过集线器直接连接两台计算机的网卡)，或者在进行集线器级联时使用，例如，用于连接两个没有“级联口”的集线器(4 口或 8 口)上的普通口。

4. 网卡的安装、设置与连接

① 安装网卡　在各工作节点上安装网卡，比如要在服务器(server)和各计算机工作站(workstation)端安装网卡，一般只需将网卡插入计算机主板中的相应槽位中，例如，将 PCI 网卡(台式计算机)或 PCMCIA 网卡(笔记本)插入相应的插槽中。注意：应在断开计算机电源的状态下进行操作，还要注意消除自身的静电，可以使用消除静电的专用装置，如手腕佩带防静电的操作环，并站在防静电的小块地毯上等。

② 在代理服务器端安装 ISDN 卡　安装方法与安装网卡的方法类似。

③ 连接网线　按照图 16-1 所示的网络结构，使用标准线分别连接各计算机的网卡到集线器或交换机上。

④ 设置网卡硬件参数　使用网卡自带的驱动程序(通常为 DOS 下的一组程序)设置好网卡的参数，并记录在案。其中，最关键的两个参数是网卡的“I/O 地址”和“IRQ(中断请求)”，一定注意不能与本机中的其他硬件参数相同。利用上述程序还可以检测网络的连通性。

至此，此办公室的 10/100Base-T 网络的硬件部分已经设计、安装和连接完毕，以上的各步，也是一个小型网络的管理员在建立、安装和组建网络初期的主要工作。

5. 软件系统的主要名称和软件清单

根据系统的设计列出所需要的软件清单如下：

① 服务器端使用的软件(如果只组建工作组网则无此项)　Windows NT Server 4.0 可以完成主域控制器、资源访问控制、身份识别、远程访问服务器、WWW 服务器、DNS 服务器和 Internet 信息服务器等多项功能。

② 代理服务器(proxy server)软件　微软的代理服务器、WinGate 或 SyGate 等专用代理服务器软件。

③ 各计算机工作站(或客户端)的软件　如果是工作组方式，则使用 Windows 98；如果是域工作方式，则使用 Windows NT Workstation 4.0，完成系统要求的功能。

④ 使用路由器自带管理软件或者是 ISDN 卡自带的软件，完成接入 Internet 的功能。

⑤ 数据库软件　SQL Server 软件。

⑥ 浏览器软件　IE 5.5 或 Netscape 4.6。

⑦ 其他软件根据情况选择。

6. 使用 Windows 95/98/Me 组建小型办公室的工作组网络

在小型办公室中，计算机的桌面操作系统一般使用 Windows 95/98/Me 或者是 Windows 2000 Professional，利用其内置的网络功能可以很容易地组建起自己的对等网，或者是具有一定安全和管理功能的 Windows NT Server 的域方式网络。这两种网络都具有设置简单、管理容易、使用方便和速度快等特点。除此之外，后者还具有更高的可靠性、安全性和可管理性。

由于本案例较为简单，仅要求实现网络资源的共享和 Internet 的连接共享，所以可采

用 Windows 95/98/Me 组建对等网，并实现其要求的功能。下面开始详细介绍组建对等网的方法和步骤。

首先，应当检查所使用的网络硬件是否已经连接好，Windows 操作系统是否已经正常安装运行，然后即可在 Windows95/98/Me 下配置网卡、协议等与网络相关的信息。

(1) 在 Windows 95/98 下添加并设置网卡

对于 ISA 网卡，在 DOS 下使用网卡自带的驱动程序设置和检测之后，还要到各种工作站的操作系统(例如 Windows 95/98/Me)下进行网卡的添加和设置。计算机上设置的网卡参数值应以 DOS 下设置的参数为准。而对于 PCI 网卡一般只需在 Windows 95/98/Me 下进行安装。在 Windows 95/98/Me 下添加、设置网卡的步骤如下：

① 依次选择“开始”→“设置”→“控制面板”命令选项，在打开的窗口中双击“网络”图标，激活“网络”窗口，打开“配置”选项卡。

② 在“网络”窗口的“配置”选项卡中，单击“添加”按钮，激活如图 16-3 所示的“选定网络组件类型”窗口。



图 16-3 “选定网络组件类型”窗口

③ 在“选定网络组件类型”窗口中，选中“适配器”，单击“添加”按钮。

④ 在“选定网络适配器”窗口中，选择网卡的制造厂商和型号等。选好之后，单击“确定”按钮，返回“网络”的“配置”窗口。

⑤ 应注意根据所添加的网卡类型进行选择，如果列表中没有拟添加的网卡，则应单击“从磁盘安装”按钮，并使用网卡提供的驱动盘进行安装。如果是 ISA 网卡，此处选择和设置的参数值应当与 DOS 下网卡驱动程序中设置的值一致。

⑥ 在“网络”窗口中的“配置”选项卡中，先选择所安装的网卡，然后单击“属性”按钮，激活如图 16-4 所示的窗口。

⑦ 在图 16-4 所示的窗口中，单击“资源”选项卡，从中选择可以配置的“I/O 地址范围”等信息。设定后，单击“确定”按钮，重新启动计算机，使设置生效。至此，网卡的设置过程结束。

(2) 设置用户的常规信息

① 依次选择“开始”→“设置”→“控制面板”命令选项，在打开的窗口中双击“网络”图标。

② 在弹出的“网络”窗口中，选择“标识”选项卡，激活如图 16-5 所示的窗口。在此窗口中，可以设置和修改用户计算机和工作组的名称，同一工作组的工作组名应当一致，而计算机名应当各不相同。

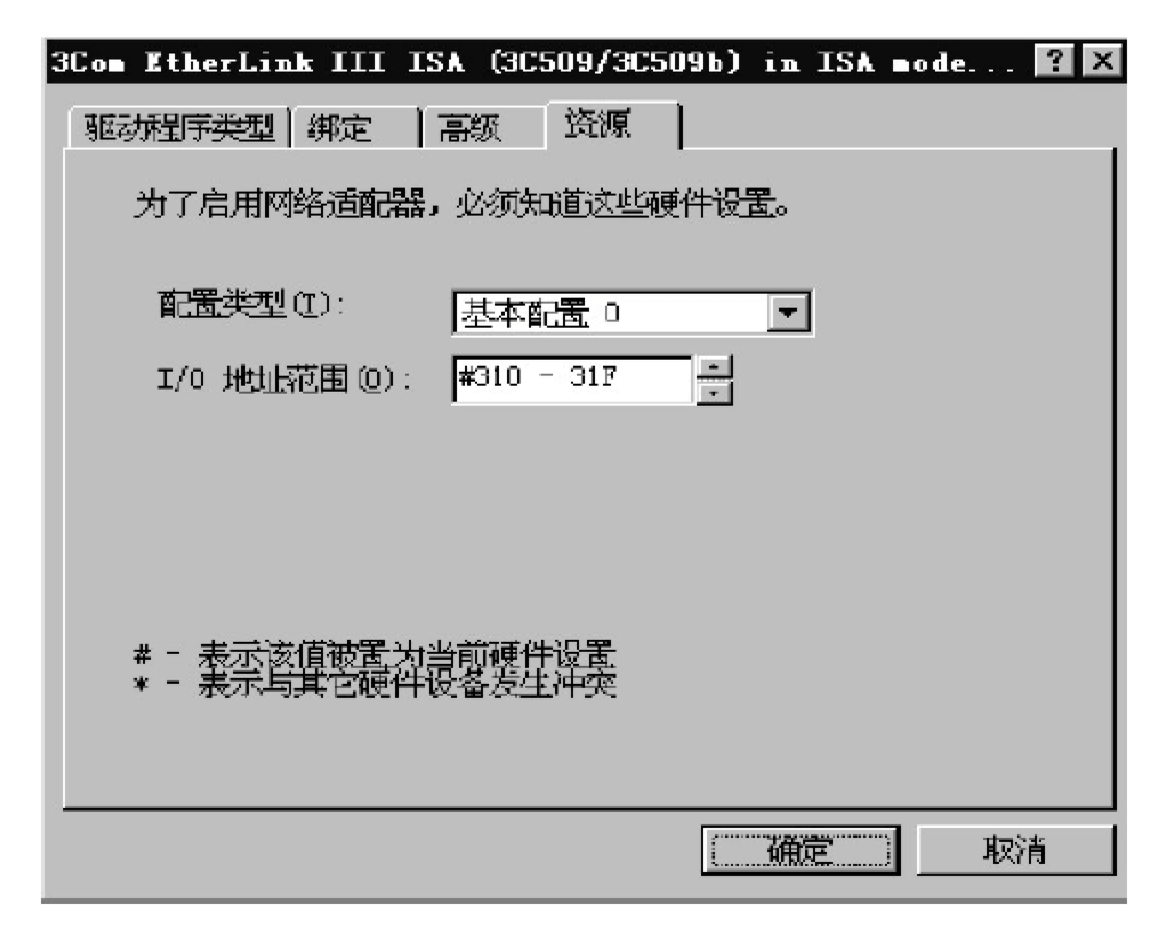


图 16-4 选定网卡的“资源”选项卡设置窗口

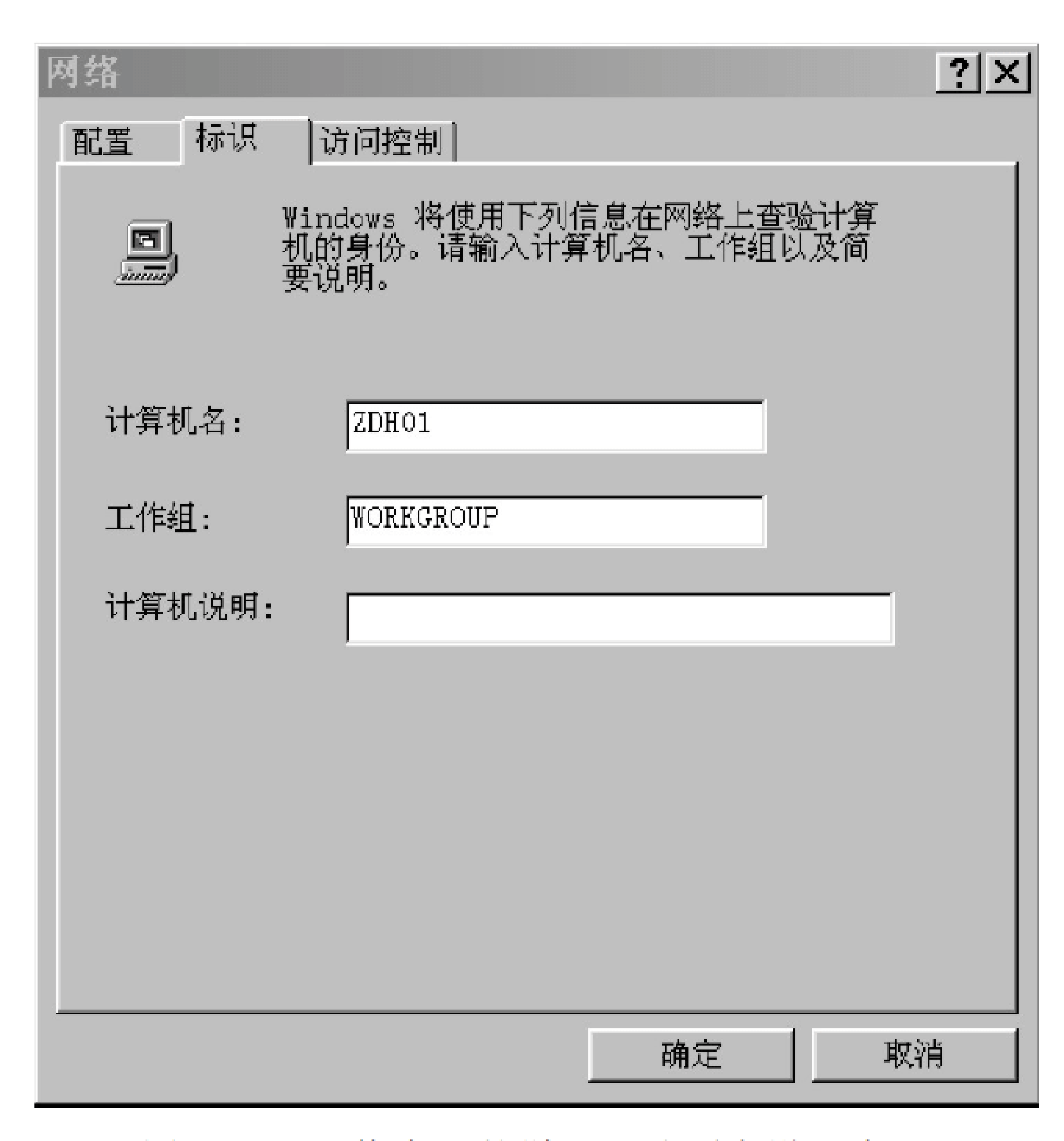


图 16-5 网络窗口的“标识”选项卡设置窗口

(3) 选择用户操作类型

① 在“网络”窗口中，选择“配置”选项卡，单击其中的“添加”按钮，激活如图 16-3 所示的窗口。

② 在图 16-3 所示的“选定网络组件类型”窗口中，选择“客户”选项后，单击“添加”按钮。在激活的“选定网络客户”窗口中，显示了 Windows 95/98/Me 支持的多个厂家的多种网络结构，可根据自己的情况酌情选择。在窗口左侧选择 Microsoft，在窗口右侧单击“Microsoft 网络客户”，最后单击“确定”按钮。

(4) 选择和设置网络通信协议

在 Windows 95/98/Me 中添加与设置协议的步骤如下：

① 在“网络”的“配置”选项卡中，单击“添加”按钮。

② 在激活的图 16-3 所示的窗口中，选择“协议”选项后，单击“添加”按钮，激活如图 16-6 所示的“选择网络协议”窗口。



图 16-6 “选择网络协议”窗口

③ 在“选择网络协议”窗口中，在左侧“厂商”列表中选取 Microsoft，并在右侧窗口的“网络协议”列表中选择适当的协议。例如，依次选择“NetBEUI”、“IPX/SPX 兼容协议”和“TCP/IP”等协议后，单击“确定”按钮。注意，对于那些使用 TCP/IP 协议的网络还需要进行协议的配置。

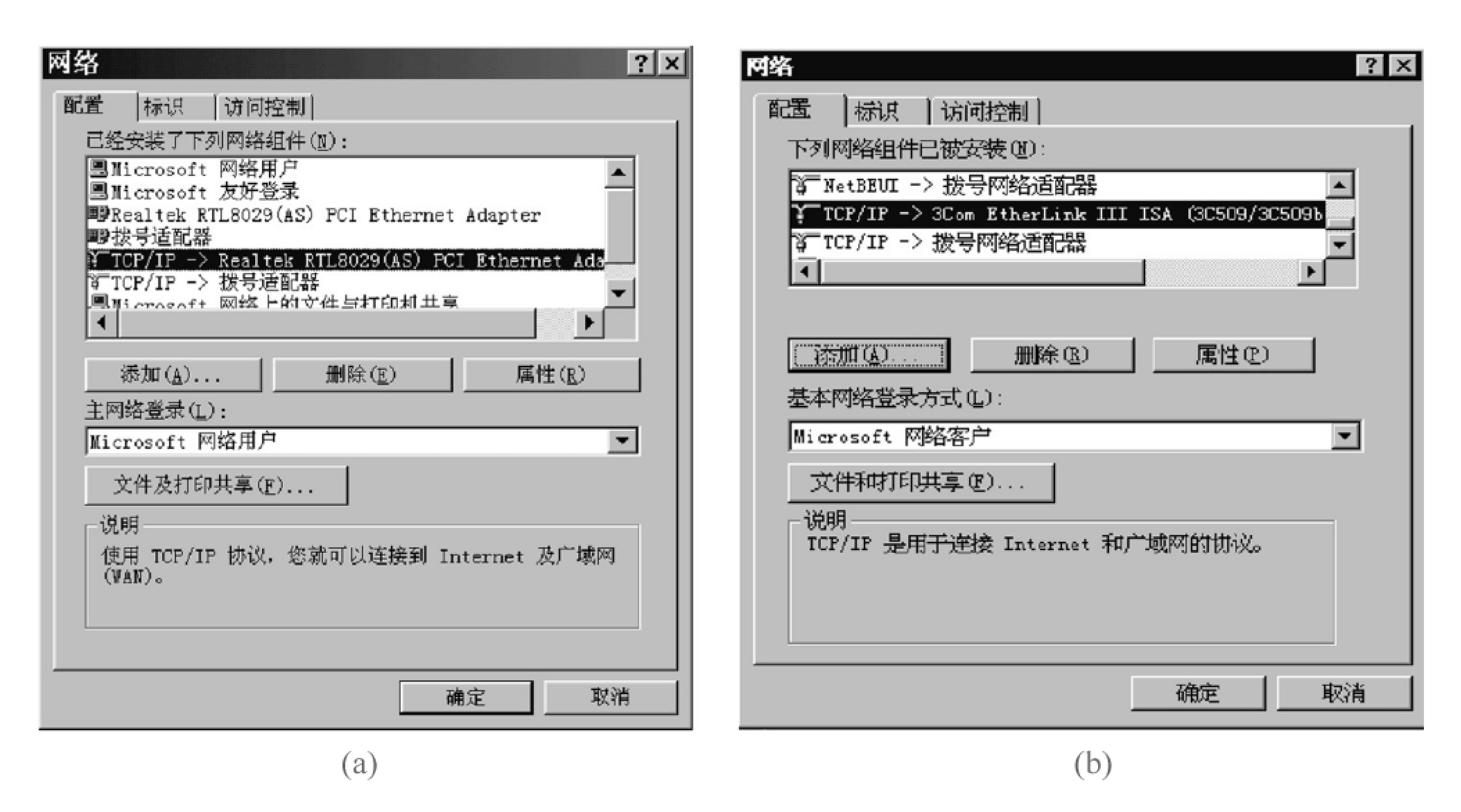
④ 配置 TCP/IP 协议时，在“控制面板”中，双击“网络”图标，在打开的“配置”选项卡中，选择需要设置的协议，例如，选择 TCP/IP→3Com Ethernet III ISA…。

注意：其一，此处的 TCP/IP 协议应该针对所使用的网卡，参见图 16-7(a)和图 16-7 (b)，如果有多块网卡，应该对每个网卡分别进行配置；其二，应当针对所选的协议进行设置，例如，如果在图 16-6 所示的窗口中，添加的是“IPX/SPX 兼容协议”或者“NetBEUI”协议，则基本不用做什么设置，如果选择的是“TCP/IP”协议，则必须设置 IP 地址和子网掩码(即子网屏蔽或 subnet mask)等参数。

⑤ 选择 TCP/IP 协议后的设置步骤如下：先在图 16-7(b)中，选择你要设置的网卡，例如，选中 TCP/IP→3Com EtherLink III ISA(3C509/3C509b)选项(此处表示针对“3 Com…网卡”配置 TCP/IP 协议)后，单击“属性”按钮，激活如图 16-8 所示的窗口。

⑥ 在“TCP/IP 属性”窗口中，选择图 16-8 所示的“IP 地址”选项卡，选中其中的“指定 IP 地址”单选项，还应该键入分配给本计算机的 IP 地址和子网掩码，例如“202.112.144.10”及“255.255.255.0”，最后，单击“确定”按钮，系统要求重新启动。

注意：同一个子网内，所有计算机 IP 地址中的“网络编号”和“子网掩码”部分的值都应该相同，而每个计算机的“主机编号”都应当不相同。例如，实例中的网络编号为“202.112.144”，子网掩码为“255.255.255.0”。该计算机的“主机编号”为“10”，配置网络中其他计算机时，这个编号应该不同。如果使用的是路由器，则各计算机需将网关地址设置为路由器的 IP 地址。如果使用了代理服务器，其它计算机则应将网关地址配置为连接



(a) (b)

图 16-7 “网络”→“配置”→“TCP/IP 协议”选择窗口

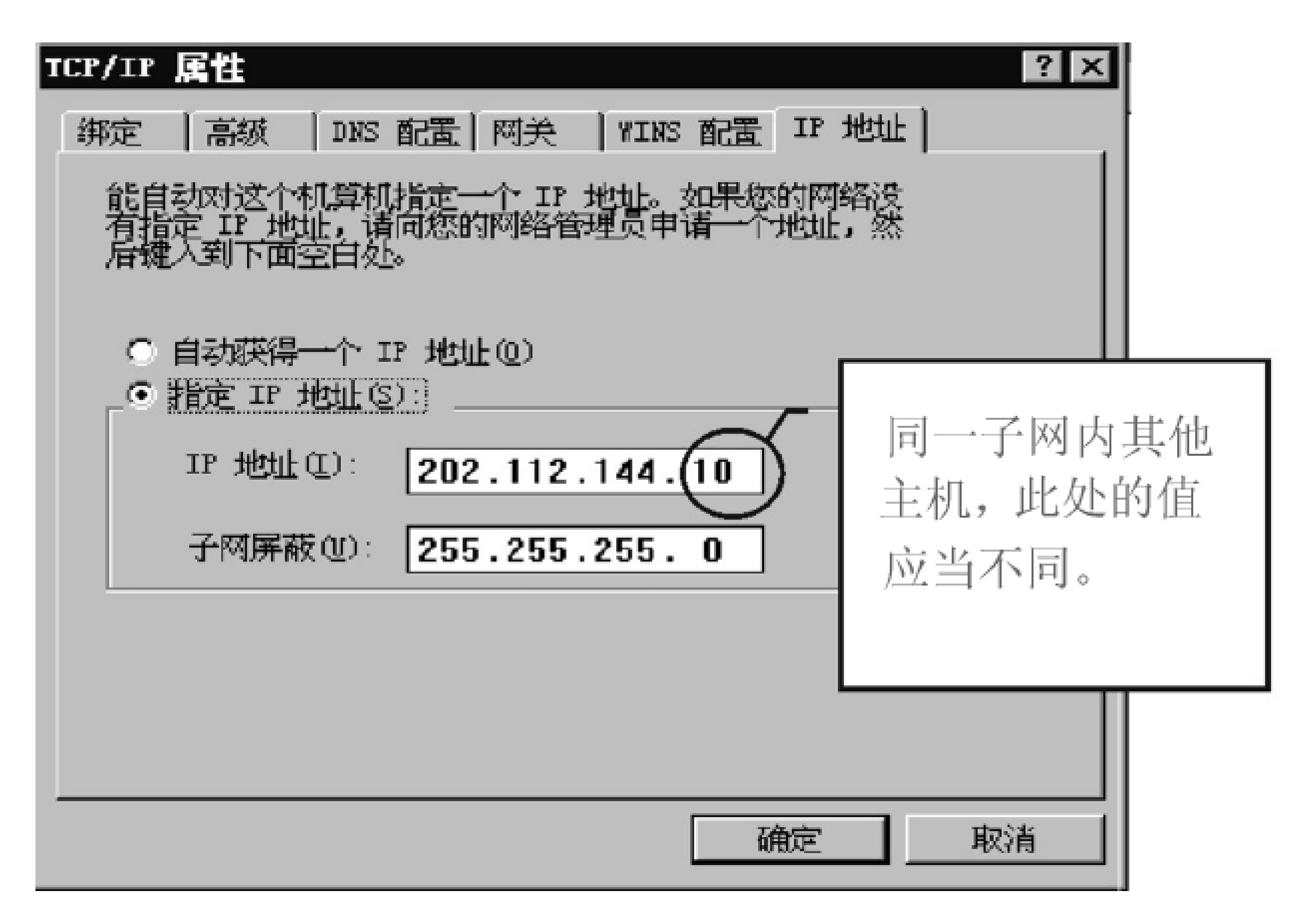


图 16-8 “TCP/IP 属性”设置窗口

代理服务器的网卡所配置的 IP 地址。

⑦ 在 Windows 95/98/Me 的桌面上双击“网上邻居”图标，检查是否正确连接。

至此，在各计算机中的网卡和 TCP/IP 协议的安装已经完毕，如果有问题可参照上述步骤依次检查网卡、网卡驱动程序、网络协议等各项内容。例如，可以分别检测如下内容：

- 检查硬件连接故障，观看集线器和交换机上的指示灯，并使用测试、管理的专用软件工具等确定和排除硬件故障。
- 检查网卡驱动程序安装是否正确。
- 检查协议是否安装正确。例如，使用 ping 命令检测 TCP/IP 协议的安装和网络的连通性。
- 检查各种工作站是否已正确加入到组或域。

7. Windows 95/98/Me/NT 计算机上开放和使用共享资源

在 Windows 95/98/Me 计算机上，开放和使用共享资源的方法都分为两步。第一

步，在开放资源的计算机的“资源管理器”中，直接设置拟开放的共享资源；第二步，在使用资源的计算机中，可以在“网上邻居”中直接使用共享资源，当然，也可以使用“映射网络驱动器”的方法来共享资源。

8. 远程访问服务和共享接入 Internet

（1）选择和确定接入 Internet 的方式

本案例局域网的规模较小，因此，可以选择和使用 ISDN 专线的方式接入 Internet。由于每条 ISDN 可以提供 128Kb/s 的因特网访问速度，因此，如果带宽不够，可以租用 2 条 ISDN 专线。

（2）确定接入设备

在代理服务器上使用 ISDN 卡，或者选择相应带宽的 ISDN 路由器接入 Internet。

（3）确定远程访问接入服务系统

使用 Windows NT Server 4.0 中的 RAS 服务器完成远程工作站的接入访问工作。

（4）确定代理服务系统

① 代理服务器端　可以使用微软 IE 的代理服务器（Proxy Server）软件，或者使用专用的代理服务器软件 WinGate 等代理局域网内的用户接入 Internet。

② 代理服务器的客户机端　在 Windows 95/98/Me 上可以使用内置的 TCP/IP 协议软件，设置其网关地址为代理服务器网卡使用的 IP 地址。另外，可使用微软的 IE 浏览器进行信息资源的访问，使用 Outlook Express 收发电子邮件。

9. 调试各服务子系统的功能

进行系统的联合调试实现原定的系统功能目标，如资源访问控制系统、身份识别系统、DNS 服务系统、WWW 服务系统、远程访问服务系统和 Internet 信息服务系统等各项子系统的功能。

10. 制作合理的备份计划及故障后的备份恢复

本案例所做的备份计划如下：

- 每月末做一次整体备份　系统安装之后，先做一次系统磁盘的整体备份，以后每个月末做一次整体备份，使用光盘和磁带存储。
- 每周（末）做一次差量备份　网络用户数据文件和网络用户账号与属性的差量备份，使用磁带和硬盘存储。
- 每日（下班之后）做一次系统的增量备份　存储上一次整体备份或增量备份以来的所有变化了的文件，使用磁带和硬盘存储。
- 归档备份　随时按用户的特定要求做好 3 个指定的归档备份，使用活动硬盘和光盘存储。
- 无日常备份。
- 备份的数量和存放位置　使用 3 盘磁带循环存储。分别存放在两个不同的安全地带。

在所备份的系统出现故障时，应当以使用户的数据损失最少为原则，正确使用已有的备份进行系统、用户数据或指定目录文件的恢复。

实例：对于本例做作的备份计划，如果在运行 3 个月之后的某月的第 3 周的第 3 天，

系统崩溃，请简述使用哪些备份进行系统恢复可以使得用户的损失最少。

实例解题步骤要点：

(1) 分析用户在发生故障之前应当具有的备份

- 上个月末的系统磁盘的整体备份；
- 发生故障前两周的差量备份；
- 发生故障前两天的增量备份；
- 用户在最近要求作过的归档备份。

(2) 使用上述备份手段恢复系统和用户数据

- 使用原有的备份程序恢复上个月末系统磁盘的整体备份；
- 使用原有的备份程序恢复故障前最近一周末做过的差量备份；
- 依次恢复发生故障前两天的增量备份；
- 根据用户的要求恢复指定的归档备份。

16.3 网络管理员在网络管理中的职责综述

无论多么先进的网络都是由人参与管理的，因此，网络管理员在整个网络中具有不可替代的作用。与其他机构的管理者一样，网络管理员也有着具体的职责和必须遵循的原则。网络管理员只有忠于自己的职责，并遵循相应的原则，才能确保网络正常、安全、可靠地运行。当网络安全受到损害或出现问题的苗头时，网络管理员应具有紧急情况下处理故障的能力，并能够作出相应的判断，采取合理的措施。

通过上述案例和本书的学习，可以看到，网络管理员是指为了实现一个网络系统所设计的功能，负责网络的安装、维护和故障检修等工作，并能够使网络正常运转的一名或多名专业人员。虽然每个网络管理员所管理的网络的规模、结构、复杂程度和具体任务要求各不相同，但是网络管理员应当完成的基本任务还是有共同和相似之处的，本节就对这些任务作一综述。

1. 网络系统的硬件的安装与维护

根据网络的设计进行的网络硬件安装与维护工作包括：网络工程早期的确定、布线、组网和调试；工程完成之后的日常硬件的维护，如调整、新增服务器或工作站、扩充部件(如内存、硬盘)、查找并替换已损坏的网络部件(如网线、网卡)。这部分的工作是十分繁琐却又经常发生的，现将常规的硬件管理工作归纳如下：

① 硬件的安装　包括组建网络、工程布线、网络设备的安装，例如，网络打印机、交换机、路由器、不间断电源、大型贵重共享设备等的安装。

② 硬件的维护　包括根据公司人员和工作的变动情况增加新的服务器和工作站；扩展计算机的内存和硬盘；更换破损的网络电缆、网卡、网络设备和网络共享设备等多种日常维护工作。

2. 网络服务器的安装、配置与维护

网络服务器和客户工作站的安装与维护工作是组建和管理 Intranet 或其他网络的核

心与关键。在实际的管理与维护工作中，首先要让系统设计的各个服务子系统正常地运行起来，并负责它们的日常维护与管理工作，确保信息高速公路的畅通和信息服务的正常运行；其次，是维护和更新各个子系统。

对中小企业的网络管理员来说，需要配置的服务器有接入服务器，DNS服务器，Web服务器，邮件服务器和文件服务器。Intranet中需要安装和配置的各类网络服务器如下所述：

（1）网络服务器的早期安装工作

① 网络控制服务器　是指安装网络操作系统的中心控制服务器，例如NT/2000中的“主域控制器”，Novell网络的文件服务器等。

② WWW服务器　例如IIS 4.0/5.0中的WWW服务器。

③ FTP服务器　例如IIS 4.0/5.0中的FTP服务器。

④ 数据库应用服务器　例如SQL Server等。

⑤ 电子邮件服务器　例如Exchange Server等。

⑥ 域名服务器　例如NT中的DNS服务器。

⑦ 打印服务器　网络打印机的组织与安装，例如NT中打印机池的安装和配置。

⑧ 动态主机配置协议服务器　例如NT中的DHCP服务器。

⑨ 远程访问服务器　例如NT中的RAS服务器。

（2）网络服务器的日常维护工作

① 上述各种服务器的日常维护工作。

② 更新WWW服务器的页面信息。

③ 维护、注入和更新数据库服务器中的数据

④ 管理电子邮件服务器的用户信箱等。

⑤ 备份与恢复系统备份。

由于网络的规模、功能和安全性能各不相同，因此，网络中需要管理的网络服务器也不相同。网络管理员应当根据自己管理的网络的具体情况，进行安装和维护。安装之后，并不意味着万事大吉，真正艰苦和大量的工作还在后边。例如主域控制器管理的服务，计算机和账户的不断维护和更新，WWW服务器页面的维护与更新，数据库数据的注入、备份与保护，邮件服务器用户信箱的管理等。因而，许多公司和企事业单位都专门成立了网络信息中心专门负责这些任务。

3. 网络客户工作站的安装与维护

网络工作站就是网络客户使用的计算机，简称工作站或客户机。网络工作站是网络客户的前端窗口，用户通过它访问网络中的共享资源和网络服务，当网络客户不能正常使用网络服务和网上的共享资源时，自然会求助于网络管理员。因此，网络客户机的安装和配置是工作站的起始管理工作，而其日常维护工作才是网络管理员的一项经常性的工作。网络客户工作站的安装、配置与维护工作有以下几项：

① 网络工作站硬件的安装与配置　其开始时的工作应当同与其对应的服务器的安装和配置工作一起完成，例如，配置邮件服务器之后，就进行工作站的配置，最后进行服务器/客户机的联合调试。

② 网络工作站上各种应用软件的安装和配置　例如用户使用的常用办公软件、工具软件等。

③ 网络工作站与各种网络服务器的互联　例如，安装网络操作系统的客户端系统软件 NT Workstation、Windows 98，或 DOS 等，然后进行联网的调试。

④ C/S 或 B/S 模式的网络应用系统中客户端软件的安装与维护　例如，安装 WWW 服务器的客户端软件 IE。

⑤ 客户工作站上共享资源与非共享资源的管理　例如工作站上客户资源的管理。

⑥ 网络工作站故障的诊断与排除　例如，当网络工作站出现故障时的诊断与排除。

⑦ 工作站安全系统的安装与管理　例如，采用工作站防病毒软件，对工作站进行定时杀毒或实时监控等。

4. 应用软件的维护

应用软件的维护是指在网络上安装用于共享的应用程序，删除无用的程序，以及升级软件等大量琐碎的日常的软件维护工作。例如，安装和维护图形软件、办公软件、杀毒软件和各种工具软件，升级 Office 和 Photoshop 等。

5. 网络用户管理

网络用户管理是网络管理员的另一项重要和经常性的工作，也是保证网络安全和可靠运行的重要措施。

网络硬件系统建成后，网络管理员要完成的首要工作就是进行“组”或“域”工作方式的选择、设计；然后，按照设计的组织方式建立各个域或组内的用户账户、密码，并设置它们对网络的访问权限。此外，网络管理员应针对网络各部门人员和工作的变动情况，及时地进行必要的网络用户管理工作，例如当用户所属的组或用户账号本身变化时需作的更改工作。网络用户管理工作主要包括以下几个部分：

① 为每个用户（员工）设置账户、密码，并分配适当的访问网络的权限；还应根据变动情况及时地进行更新、备份和调整工作。例如，为了确保网络的安全，应定期更换密码。

② 为了管理方便，网络管理员应当对每个用户和部门进行精心的组织，建立起“组账户”，并尽量使用“组账户”对用户进行统一的管理。

③ 为不同的用户和组使用的网络资源设置必要的访问权限，限制非法用户的访问。

④ 为系统开放的共享资源设置安全的访问控制权限。

6. 网络目录和文件系统的管理

网络中目录和文件系统的管理是非常重要的一项工作。这是因为，网络中所有的系统文件、应用程序、数据资料和用户使用的文件都是以目录和文件的形式存放在各种存储介质上的，例如，存放在软盘、硬盘、磁带和光盘等介质上。一旦这些数据被损坏，轻则影响企业工作的正常进行，重则造成不可估量的毁灭性损失。因此，对网络中的目录文件必须具有完备的备份、管理和维护措施。网络管理员对网络目录和文件的常规管理工作有以下几种：

① 应当根据实际工作的需要选择和确定文件系统的格式。例如，在 Windows NT 和 2000 中可以选择的有 FAT 和 NTFS 格式。如果系统要求更高的灵活性，则应选择前者；如果数据的安全更为重要，则应采用后者。因此，对学校等一般安全性要求的网络可以选

择前者，而对于公司、企事业等对安全要求较高的单位，就应选择后者。

② 应当制定出完备的数据保护制度。

③ 对重要的数据目录和文件应作定期的备份。

④ 发生故障时对数据目录和文件进行恢复。

综上所述，网络中的各种信息资源是网络中最重要的保护资源，而这些资源都是以文件和目录的形式存放在介质中的，因此，网络管理员日常的一项重要工作就是维护（备份和恢复）共享资源的文件和目录。网络文件与数据备份的目的就是为了在需要时，能够及时恢复文件和目录中保存的数据。

7. 网络打印设备的组织和日常管理

网络打印机负责网络中各种文件和资料的打印，通常打印设备的共享是网络组建的基本目的之一。在网络中，网络打印机（打印设备）和其他硬件设备都可以通过网络提供给其他用户使用。在网络打印设备共享和使用之前，网络管理员需要对网络打印设备进行组织。因为，只有设计合理的打印系统，才能发挥出网络打印设备的最大功效。网络管理员对网络打印设备的日常管理主要有以下几个方面：

① 对网络打印设备进行合理的组织，选用和设计适宜的网络打印系统。例如，将相同的若干台打印设备组织为一个“打印机池”。这样用户可以通过使用同一个名称，来使用这一组打印设备，打印机池中各个设备的分配和使用可以由系统自动控制。

② 设计好之后，网络管理员应当完成网络打印服务器的安装和配置，并将服务器的打印设备设为共享状态，供网络上的其他用户使用。例如，可以充当打印服务器的平台有：NT Server、NT Workstation、Windows 95/98/2000 以及 DOS 工作站。

③ 根据工作站性质的不同，在工作站上进行网络打印设备的安装和设置。

④ 打印设备的日常维护。主要包括各个网络打印机软、硬件的维护。例如，更换打印设备的耗材和易损部件。

⑤ 根据用户需求合理地安排打印作业，维护打印服务器的正常运行。例如，增加新的打印设备、删除故障打印机、进行打印作业的组织管理等，如为不同用户设置或调整打印的优先级和打印时段。

网络打印设备的管理是企事业单位办公自动化中的重要组成部分。网络管理员在此部分的具体工作和操作管理技巧，请参见第 11 章。

8. 网络管理软件的安装、运行和维护

在中小型的网络中，网络管理员通常借助于网络操作系统中内置的管理工具，辅以其他管理软件对网络进行管理，因此，管理行为的主体常常是网络管理员。而在大、中型网络中，网络管理员应当能够运用网络管理软件，对网络实行自动的监控和管理。例如，使用 HP 公司的 OpenView、IBM 公司的 NetView 或 SUN 公司的 SunNet 等软件对网络进行管理。使用这些软件时，应注意配备具有网管功能的网络设备。例如支持 SNMP 协议的交换机。

9. 网络性能的管理与提高

根据网络性能和故障的状况，及时进行网络诊断、排除故障，调整系统性能。例如，网络管理员可以设置系统性能的报警，当硬盘空间不足时自动报警或通知有关账户。

10. 网络中的安全管理工作

网络管理员应当根据网络安全指标的要求,采用各种安全技术和安全措施,确保网络数据的可用性、完整性和保密性。安全管理的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。一旦发生异常,网络管理员应当有能力做出判断,采用必要的手段和措施,阻止网络上发生的非法攻击,并及时恢复网络系统和用户数据,使得网络数据的损失降低到最小。

(1) 可能受到威胁的网络资源

① 硬件设备:例如服务器、交换机、路由器、集线器和存储设备等。

② 软件系统:例如操作系统、应用软件和开发工具等。

③ 数据或信息。

(2) 网络管理员可采用的网络安全保护措施

① 物理措施:对交换机、路由器、大型计算机等网络关键设备,制订并执行严格的规章制度,采取有效的防辐射、防火等物理措施。

② 访问控制:对用户登录网络和网络资源的访问权限进行严格的认证和控制。

③ 数据加密:通过对网络中传输的数据进行加密来保障网络资源的安全性。

④ 防止计算机病毒:计算机病毒对计算机网络的危害越来越大,并且可以带来直接或间接的巨额经济损失。因此,防止计算机病毒是网络系统设计中必须考虑的问题之一,应该从服务器和工作站两方面入手,来防止计算机病毒的入侵。

⑤ 其他措施:主要包括容错技术、数据镜像、数据备份和审计等。

11. 网络维护

实际上网络管理与维护是一项复杂的工作,除了前面各章中介绍的各章的管理之外,网络管理员还需要解决许多综合性的实际问题。因此,若要管理好一个更大的网络,除了必要的理论知识外,还需要大量长期的实际操作,才能取得网络维护的具体经验。

在使用 Windows NT 实现和管理一个具体的 Intranet 时,有关网络管理员在每一部分中的具体职责和实现技术已在本书中的各章做了详细的介绍。相信通过本书的理论和实验环节的学习,读者应当可以搭建起一个具有中型规模的、使用浏览器进行信息资源访问的 Intranet,并能够初步掌握作为一个初级网络管理员应具备的基本知识和技能。

习题

(1) 网络管理员的责任是什么?应当遵循哪些原则?

(2) 网络管理中的重点和难点是什么?具体工作又是什么?

(3) 网络中常见的故障有哪些?

(4) 网络管理员的职责是什么?所要做的主要工作有哪些?

(5) 网络管理员在网络硬件的安装与维护工作中应当做些什么?

(6) 网络服务器和客户工作站的安装、配置与维护是指什么?用户管理的内容是什么?

(7) 应用软件的维护工作有哪些？请举例说明。

(8) 为什么强调网络目录和文件系统的管理的重要性？

(9) 网络打印设备的组织和日常管理工作有哪些？

(10) 可能受到威胁的网络资源有哪些？网络管理员可采用的网络安全保护措施有哪些？

(11) 如果本章案例中的系统正常运行半年后，在某月的第 4 周的第 4 天系统崩溃，请简述使用哪些备份进行系统恢复可以使得用户的损失最少。

实训题目

1. 制作 3 类或 5 类 UTP 网线连通网络硬件

- 按照本章介绍的方法，制作标准线或交叉线。
- 在计算机中安装网卡。使用所做的网线连接集线器和网卡。

2. 网卡安装实验

- 对于 ISA 网卡，使用网卡的 DOS 安装盘，完成网卡在 DOS 下的安装和检测任务，记录网卡的参数：IRQ 和 I/O。
- 对于 PCI 网卡，在 Windows 98/Me 下，在控制面板中添加和安装网卡，记录 Windows 98/Me 下的网卡的类型和参数(IRQ 和 I/O)。

3. TCP/IP 协议的安装和检测实验

- 选择并打开 Windows 98/Me 的“控制面板”中，激活“网络”窗口，添加和配置 TCP/IP 协议，记录自己主机的 IP 地址。
- 在 DOS 环境窗口：使用 ping 命令测试 TCP/IP 协议设置的正确性，以及网络的连通性。

4. 对等网设置和连接实验

按本章介绍的设置和连接要点完成两台或多台 Windows 95/98/Me 工作站之间“工作组”方式互联的操作。

5. 共享资源的开放和使用

在资源所在计算机上，选择欲开放的资源目录，单击鼠标右键，选择“共享”命令选项，在打开的窗口设置共享名，添加共享目录的访问权限。

参 考 文 献

[1] 尚晓航.计算机网络技术教程.北京:人民邮电出版社,2001
[2] 尚晓航.网络系统管理——Windows NT 篇.北京:人民邮电出版社,2002
[3] 尚晓航.计算机局域网与 Windows NT 实用教程.北京:清华大学出版社,1999
[4] 黄叔武,杨一平.计算机网络工程教程.北京:清华大学出版社,1999
[5] 夏功宜,吴英.计算机网络基础.天津:南开大学出版社,1998
[6] 陈明.Windows NT 应用技术 500 问.北京:科学出版社,2000
[7] 吴万泉.局域网组建实例与应用.北京:人民邮电出版社,2001
[8] 戴有炜编著.王明华,王燕改编.Windows NT Server 4.0 中文版实用指南.北京:清华大学出版社,1997
[9] [美]Anil Desai 著.虞里平,胡昌浩译.Windows NT 低成本网络管理.北京:电子工业出版社,2000
[10] 张琳.网络管理与应用.人民邮电出版社,2000
[11] 黎洪松,裘晓峰.网络系统集成技术及应用.北京:科学出版社,1999
[12] 楚狂.网络安全与防火墙技术.北京:人民邮电出版社,2000